

THE GOLDBACH'S CONJECTURE PROVED

AGOSTINO PRÁSTARO

Department SBAI - Mathematics, University of Rome "La Sapienza", Via A.Scarpa 16, 00161
Rome, Italy.

E-mail: agostino.prastaro@uniroma1.it

ABSTRACT. We give a direct proof of the *Goldbach's conjecture*, (GC), in number theory, in the Euler's form. The proof is also constructive, since it gives a criterion to find two prime numbers ≥ 1 , such that their sum gives a fixed even number ≥ 2 . The proof is obtained by recasting the problem in the framework of the Commutative Algebra and Algebraic Topology. Even if in this paper we consider 1 as a prime number, our proof of the GC works also for the *restricted Goldbach conjecture*, (RGC), i.e., by excluding 1 from the set of prime numbers.

AMS Subject Classification: 11R04; 11T30; 11D99; 11U05; 81R50; 81T99; 20H15.

Keywords: Goldbach's conjecture; Algebraic number theory; Diophantine equations; Quantum algebra; Cobordism groups; Integral cobordism groups of quantum PDEs; Crystallographic groups.

1. Introduction

*"Every even integer is a sum of two primes.
I regard this as a completely certain theorem, although I cannot prove it."
(Euler's letter to Goldbach, June 30, 1742.)*

The well known Goldbach's conjecture in number theory, remained unsolved up to now, was one of the most famous example of the Gödel's incompleteness theorem [4, 5, 6, 8]. In this paper we give a direct proof of this conjecture. Some useful applications regarding geometry and quantum algebra are also obtained.

Our proof is founded on the experimental observation that fixed an even integer, say $2n$, $n \geq 1$, and considered the highest prime number $p_1 \in P$, that does not exceed $2n$, the difference $2n - p_1$ is often a prime number, or if not, we can pass to consider the next prime number, say $p_1^{(1)} < p_1$, and find that $2n - p_1^{(1)}$ is just a prime number. (We denote by P the set of prime numbers.) Otherwise, we can continue this process, and after a finite number of steps, obtain that $2n - p_1^{(s)} = p_2^{(s)}$, where $p_2^{(s)} \in P$. This process gives us a practical way to find two primes $p_1^{(s)}$ and $p_2^{(s)}$, such that $2n = p_1^{(s)} + p_2^{(s)}$, hence satisfy the Goldbach's conjecture. In Tab. 1 are reported some explicit calculations for $2 \leq 2n \leq 998$. Here, in agreement to the original GC, we consider the number 1 as a prime number. However, our criterion works well also if the number 1 is excluded by the set of prime numbers. Of course

the question is "Does this phenomenon is a law and why?"¹ The main result of this paper is to prove that this criterion (in the following referred as "criterion in Tab. 1"), is mathematically justified. For this we recast the problem in the framework of the Commutative Algebra and Algebraic Topology, by showing that to solve the GC is equivalent to understand the algebraic topologic structure of the ring \mathbb{Z}_{2n} . In fact, the criterion in Tab. 1 is encoded by Theorem 2.20. After the proof of this theorem the GC and RGC are simple corollaries.

The paper is organized in an Introduction, where we illustrated our criterion to solve the GC, by means of algebraic topologic methods. There is also emphasized by means of a cannot-go theorem (Theorem 1.1) the difficulty to solve the GC by simply looking to the prime numbers in the ring of integers \mathbb{Z} . In Section 1 we study some fundamental properties of the rings \mathbb{Z} and \mathbb{Z}_m . The main result is contained in Theorem 2.20 that proves that criterion in Tab. 1 is justified by the algebraic topological structure of the rings \mathbb{Z} and \mathbb{Z}_{2n} . Then Corollary 2.49 and Corollary 2.50 conclude the proof of the GC and RGC too. In Section 2 are shortly given some applications of the GC respectively in the Euclidean Geometry and in Quantum Algebra and Quantum PDE's, as formulated by A. Prástaro. (For information on this last subject see [12, 13] and related works quoted therein.) More precisely, in Proposition 3.1 we recall a previous application of the GC given by [10] that now is a theorem. This relation is interesting, since it relates the GC to a diophantine equation that, now, after Corollary 2.49 and Corollary 2.50, can be considered solved too. Finally Theorem 3.2 relates the GC to the quantum algebra and algebraic topology of quantum PDEs, as formulated by A. Prástaro, showing the existence of a canonical homomorphism between the group of even quantum numbers and a suitable group related to a point group of crystallographic groups. Before to pass to the proof of above criterion, i.e., to the proof of the GC, let us emphasize by means of the following theorem, the novelty of above criterion.

Theorem 1.1 (A cannot go theorem). *In general, i.e., for any even integer $2n$, one cannot find two prime integers p_1 and p_2 satisfying the GC by simply utilizing the primality of these numbers.*

Proof. Let us prove that one cannot find two prime integers $p_1, p_2 \in \mathbb{Z}$, that satisfy the GC simply by using the fact that these numbers must be prime numbers. This can be seen by utilizing the ring structure of \mathbb{Z} . In the following lemma we resume some properties of ideals in \mathbb{Z} .

Lemma 1.2 (Fundamental properties of ideals of \mathbb{Z}). *One has the following properties for ideals of \mathbb{Z} .*

- 1) *All the ideals of \mathbb{Z} are the principal ideals $n\mathbb{Z}$, $n \geq 0$.² (These are additive subgroups of \mathbb{Z} .) One has $n\mathbb{Z} = \mathbb{Z}$ iff n is invertible, i.e., $n = 1$.*
- 2) *$n\mathbb{Z} \subset m\mathbb{Z}$, ($m \geq 1, n \geq 1$), iff $n|m$, m divides n , i.e., $n = mp$, $p \geq 1$.*
- 3) *$m\mathbb{Z}$ is a maximal ideal in \mathbb{Z} , iff m is prime.*
- 4) *The principal ideal $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, has $d = \text{g.c.d.}(m, n)$.*
- *Then we can write $d = mx + ny$, for some $x, y \in \mathbb{Z}$.*

¹The Goldbach's conjecture formulated in this way is usually called *strong GC*. This implies the following *weak GC*: "All odd numbers greater than 7 are the sum of three odd numbers". Another version of the GC is the following: "Every integer greater than 5 can be written as the sum of three primes".

²A principal ideal \mathfrak{p} of a ring R , is characterized by the property $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

TABLE 1. Criterion to find a solution to the Goldbach's conjecture:
 $2n = p_1^{(s)} + p_2^{(s)}$ con $p_1^{(s)}, p_2^{(s)} \in P$.

$n \geq 1$	$2n$	$p_1 \in P$	$2n - p_1 = p_2 \Rightarrow 2n - p_1^{(1)} = p_2^{(1)} \Rightarrow \dots 2n - p_1^{(s)} = p_2^{(s)}$
1	2	1	$2 - 1 = 1$
2	4	3	$4 - 3 = 1$
3	6	5	$6 - 5 = 1$
4	8	7	$8 - 7 = 1$
5	10	7	$10 - 7 = 3$
6	12	11	$12 - 11 = 1$
7	14	13	$14 - 13 = 1$
8	16	13	$16 - 13 = 3$
9	18	17	$18 - 17 = 1$
10	20	19	$20 - 19 = 1$
...
110	220	211	$220 - 211 = 9 = 3 \times 3 \Rightarrow 220 - 199 = 21 = 3 \times 7$ $\Rightarrow 220 - 197 = 23$
173	346	337	$346 - 337 = 9 = 3 \times 3 \Rightarrow 346 - 331 = 15 = 3 \times 5$ $\Rightarrow 346 - 317 = 29$
259	518	509	$518 - 509 = 9 = 3 \times 3 \Rightarrow 518 - 503 = 15 = 3 \times 5$ $\Rightarrow 518 - 499 = 19$
266	532	523	$532 - 523 = 9 = 3 \times 3 \Rightarrow 532 - 521 = 11$
269	538	523	$538 - 523 = 15 = 3 \times 5 \Rightarrow 538 - 521 = 17$
278	556	547	$556 - 547 = 9 = 3 \times 3 \Rightarrow 556 - 541 = 15 = 3 \times 5$ $\Rightarrow 556 - 523 = 33 = 3 \times 11 \Rightarrow 556 - 521 = 35 = 5 \times 7$ $\Rightarrow 556 - 509 = 47$
298	586	577	$586 - 577 = 9 = 3 \times 3 \Rightarrow 586 - 571 = 15 = 3 \times 5$ $\Rightarrow 586 - 569 = 17$
319	628	619	$628 - 619 = 9 = 3 \times 3 \Rightarrow 628 - 617 = 11$
320	640	631	$640 - 631 = 9 = 3 \times 3 \Rightarrow 640 - 619 = 21 = 3 \times 7$ $\Rightarrow 640 - 617 = 23$
335	670	661	$670 - 661 = 9 = 3 \times 3 \Rightarrow 640 - 659 = 21 = 3 \times 7$ $\Rightarrow 670 - 653 = 17$
350	700	691	$700 - 691 = 9 = 3 \times 3 \Rightarrow 700 - 683 = 17$
309	718	709	$718 - 709 = 9 = 3 \times 3 \Rightarrow 718 - 701 = 17$
391	782	773	$782 - 773 = 9 = 3 \times 3 \Rightarrow 782 - 769 = 13$
393	796	787	$796 - 787 = 9 = 3 \times 3 \Rightarrow 796 - 773 = 23$
403	806	797	$806 - 797 = 9 = 3 \times 3 \Rightarrow 806 - 787 = 19$
410	820	811	$820 - 811 = 9 = 3 \times 3 \Rightarrow 820 - 809 = 11$
419	838	829	$838 - 829 = 9 = 3 \times 3 \Rightarrow 838 - 827 = 11$
424	848	839	$848 - 839 = 9 = 3 \times 3 \Rightarrow 848 - 829 = 19$
436	872	863	$872 - 863 = 9 = 3 \times 3 \Rightarrow 872 - 859 = 13$
448	896	887	$896 - 887 = 9 = 3 \times 3 \Rightarrow 896 - 883 = 13$
451	902	887	$902 - 887 = 15 = 3 \times 5 \Rightarrow 902 - 883 = 19$
464	928	919	$928 - 919 = 9 = 3 \times 3 \Rightarrow 928 - 911 = 17$
481	962	953	$962 - 953 = 9 = 3 \times 3 \Rightarrow 962 - 947 = 15 = 3 \times 5$ $\Rightarrow 962 - 941 = 21 = 3 \times 7 \Rightarrow 962 - 937 = 25 = 5 \times 5$ $\Rightarrow 962 - 929 = 33 = 3 \times 11 \Rightarrow 962 - 919 = 43$
486	972	971	$972 - 971 = 1$
489	978	977	$978 - 977 = 1$
492	984	983	$984 - 983 = 1$
496	992	991	$992 - 991 = 1$
499	998	997	$998 - 997 = 1$

p_1 is the highest prime such that $p_1 < 2n$.

$p_1^{(i)}$ is the highest prime such that $p_1^{(i)} < p_1^{(i-1)}$, $i \geq 1$, $p_1^{(0)} = p_1$.

$p_2^{(s)}$ is the first number in the sequence i , $i \geq 1$, such that $p_2^{(s)} \in P$.

$P \subset \mathbb{N}$ is the set of prime numbers of \mathbb{N} .

- In particular, if m and n are coprimes, then $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ and $1 = mx + ny$. In such a case $m\mathbb{Z}$ and $n\mathbb{Z}$ are called coprime ideals.
- 5) (Intersection of two ideals) $m\mathbb{Z} \cap n\mathbb{Z} = r\mathbb{Z}$, $r = \text{l.c.m.}(m, n)$, $r \geq 1$.
- Therefore one has $m\mathbb{Z} \cap n\mathbb{Z} \neq \emptyset$, and contains mn .
- 6) (Product of two ideals) $(m\mathbb{Z})(n\mathbb{Z}) = (mn)\mathbb{Z}$.

- Therefore one has $(m\mathbb{Z})(n\mathbb{Z}) = m\mathbb{Z} \cap n\mathbb{Z}$ iff m and n are coprimes.
 - $(m\mathbb{Z} + n\mathbb{Z})(m\mathbb{Z} \cap n\mathbb{Z}) = (m\mathbb{Z})(n\mathbb{Z})$.
- 7) (Ideals quotient) $\mathbb{Z}_n \equiv \mathbb{Z}/n\mathbb{Z} \cong \{0, 1, 2, \dots, n-1\}$, $n \geq 1$.
- If n is prime then \mathbb{Z}_n is the field of the maximal ideal $n\mathbb{Z} \subset \mathbb{Z}$. Then every non-zero element $a \in \mathbb{Z}_n$ is an unit, i.e., $\exists a^{-1} \in \mathbb{Z}_n$, such that $a a^{-1} = a^{-1} a = 1$.
- 8) Let be fixed the positive integers $(n_i)_{1 \leq i \leq n}$. Then one has the canonical ring homomorphism (1).

$$(1) \quad \left\{ \phi : \mathbb{Z} \rightarrow \prod_{1 \leq i \leq n} \mathbb{Z}_{n_i}, \phi(a) = (a + \mathbb{Z}_{n_i}) \right\}.$$

ϕ is surjective iff n_i and n_j are coprimes for $i \neq j$. ϕ is injective iff $\bigcap_{1 \leq i \leq n} n_i \mathbb{Z} = \{0\}$. This condition is never verified for the ideals of $n_i \mathbb{Z}$, with $n_i \neq 0$.

9) Let $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ be the prime factorization of an integer $n \geq 1$. One has the exact commutative diagram reported in (2).

$$(2) \quad \begin{array}{ccccccc} & & & & 0 & & \\ & & & & \downarrow & & \\ 0 & \longrightarrow & n\mathbb{Z} & \longrightarrow & \mathbb{Z} & \xrightarrow{j} & \boxed{\prod_{1 \leq i \leq k} (\mathbb{Z}_{p_i^{r_i}})} \longrightarrow 0 \\ & & \parallel & & \parallel & & \downarrow \\ 0 & \longrightarrow & n\mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}_n \longrightarrow 0 \\ & & & & & & \downarrow \\ & & & & & & 0 \end{array}$$

The homomorphism j is given by $j(a) \mapsto (j_i(a))_{1 \leq i \leq k}$, where $j_i : \mathbb{Z} \rightarrow \mathbb{Z}_{p_i^{r_i}}$. In other words

$$\phi(a) = (a + p_1^{r_1} \mathbb{Z}, \dots, a + p_k^{r_k} \mathbb{Z}).$$

10) (Radical of ideal in \mathbb{Z}) The radical of an ideal $m\mathbb{Z} \subset \mathbb{Z}$ is the ideal

$$\mathfrak{r}(m\mathbb{Z}) = \{x \in \mathbb{Z} \mid x^n \in m\mathbb{Z} \text{ for some } n > 0\}.$$

Set $\mathfrak{a} = m\mathbb{Z}$. One has the following properties for the radical \mathfrak{a} .

- (i) $\mathfrak{r}(\mathfrak{a}) \supseteq \mathfrak{a}$. (\mathfrak{a} is called a radical ideal if $\mathfrak{r}(\mathfrak{a}) = \mathfrak{a}$.)
- (ii) $\mathfrak{r}(\mathfrak{r}(\mathfrak{a})) = \mathfrak{r}(\mathfrak{a})$. Therefore $\mathfrak{r}(\mathfrak{a})$ is a radical ideal.³
- (iii) $\mathfrak{r}(\mathfrak{a}(\mathfrak{b})) = \mathfrak{r}(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{r}(\mathfrak{a}) \cap \mathfrak{r}(\mathfrak{b})$.
- (iv) $\mathfrak{r}(\mathfrak{a}) = \mathbb{Z} \Leftrightarrow \mathfrak{a} = \{0\}$.
- (v) $\mathfrak{r}(\mathfrak{a} + \mathfrak{b}) = \mathfrak{r}(\mathfrak{r}(\mathfrak{a}) + \mathfrak{r}(\mathfrak{b}))$.
- (vi) If m is prime then $\mathfrak{r}((m\mathbb{Z})^n) = m\mathbb{Z}$, for all $n > 0$. ($m\mathbb{Z}$ is an example of radical ideal.)
- (vii) If $m = p_1^{r_1} \cdots p_k^{r_k}$ is the prime factorization of m , then

$$\mathfrak{r}(m\mathbb{Z}) = \langle p_1, \dots, p_k \rangle = \bigcap_{1 \leq i \leq k} \langle p_i \rangle \cong p_1 \cdots p_k \mathbb{Z}.$$

Every radical is the intersection of prime ideals containing it.

(viii) $\mathfrak{r}(m\mathbb{Z})$ and $\mathfrak{r}(n\mathbb{Z})$ are coprime ideals iff m and n are coprime numbers.

³For example $\mathfrak{r}(4\mathbb{Z}) = 2\mathbb{Z}$ and $\mathfrak{r}(2\mathbb{Z}) = 2\mathbb{Z}$.

Proof. The proof of the propositions of this lemma are standard. (See, e.g., [1, 2, 3].) \square

Let us now, take two primes $p_1, p_2 \in \mathbb{Z}$. From Lemma 1.2-4, it follows that

$$(3) \quad p_1 x + p_2 y = 1$$

for some $x, y \in \mathbb{Z}$. Multiplying both sides of equation (3) by $2n$, we get

$$(4) \quad p_1 x 2n + p_2 y 2n = 2n.$$

Then from (4) it should be possible to prove the GC if we should be able to find two prime integers \bar{p}_1 and \bar{p}_2 , such that $\bar{p}_1 = p_1 x 2n$ and $\bar{p}_2 = p_2 y 2n$. But this should imply $\bar{p}_1 | p_1$ and $\bar{p}_2 | p_2$. This is impossible for prime numbers \bar{p}_i , $i = 1, 2$. Therefore, the road to find a solution for the GC, simply by starting from two primes, is wrong. \square

2. The Proof

In order to build the proof, let us associate to any integer $n \in \mathbb{N}$ the additive group $\mathbb{Z}_n \equiv \mathbb{Z}/n\mathbb{Z}$. Let us consider the following lemmas.

Lemma 2.1. • Let $G = \langle a \rangle = \{a = a^1, a^2, \dots, a^n = e\}$ be a cyclic group of order n .⁴ One has the canonical mapping $G \rightarrow \mathbb{Z}_n$, $a^r \mapsto [r]$, $1 \leq r \leq n$, that is an isomorphism: $G = \langle a \rangle \cong \mathbb{Z}_n$.

- Every group of order p prime is cyclic and abelian.⁵
- If $G = \langle a \rangle$ is a cyclic group of order n , the equality $a^\lambda = e$ happens iff $\lambda = qn$.
- Every subgroup of a cyclic group $G = \langle a \rangle$ is a cyclic group.
- The subgroup (a^k) , $1 \leq k \leq n$, with $a^k \in G$, G cyclic group of order n , coincides with (a^d) iff $k = k'd$ and $n = n'd$. (d divides k and n .) Furthermore, the order of (a^k) is $n' = n/d$.

The element $x = a^k$ is a generator of the cyclic group $G = \langle a \rangle$, of order n , iff k and n are coprimes.⁶

Lemma 2.2 (Euler's totient function and Euler's theorem). • The number of distinct generators of a cyclic group of order n is the Euler's totient function $\varphi(n) = g.c.d.(n, k) = 1$, $1 \leq k < n$, i.e., the number of positive prime integers with respect to n , in the interval $1 \leq k < n$.⁷

⁴In a ring R , with multiplicative identity element e , a *root of unity* is any element $a \in R$, of finite multiplicative order, i.e., $a^n = e$. If \mathbb{F} is a *Galois field* (i.e., finite field, e.g., \mathbb{Z}_p , with p prime) the n -th *root of unity* of \mathbb{F} , is a solution of the equation $x^n - 1 = 0$ in \mathbb{F} .

⁵A group where every element is of infinite order, is called *without torsion*. A *group with torsion* is one where every element has finite order. In general every finitely generated abelian group G is a finite direct sum of cyclic subgroups $C_j \cong \mathbb{Z}_{\nu_j}$, $\nu_j \geq 0$. Therefore G has a *torsion subgroup* $T \equiv \oplus_{\nu_j > 0} C_j = \oplus_{\nu_j > 1} C_j$. The *free part* of G is $\oplus_{\nu_j = 0} C_j \cong G/T$. The number of summand $\mathbb{Z} \cong C_0$ in the free part of G is called the *rank* of G , and represents the maximal number of linearly independent elements in G . The numbers $\nu_j > 1$ are called *torsion coefficients* of G and can be chosen as powers of prime numbers: $\nu_j = p_j^{\rho_j}$, $p_j \in P$, $\rho_j > 0$. Two finitely generated abelian groups are isomorphic iff they have the same rank and the same system of torsion coefficients. (For complementary information see e.g., [2, 3].)

⁶In fact, one has $a^k = a^{k'd} \in \langle a^d \rangle \Rightarrow \langle a^k \rangle \subseteq \langle a^d \rangle$. On the other hand, after the *Bezout relation*, $d = \alpha n + \beta k$, $\alpha, \beta \in \mathbb{Z}$. So we get $a^d = a^{\alpha n + \beta k} = a^{\beta k} \in \langle a^k \rangle \Rightarrow \langle a^d \rangle \subseteq \langle a^k \rangle$. We can conclude that $\langle a^d \rangle = \langle a^k \rangle$.

⁷For example, the group of units of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, is $\mathbb{Z}_6^\times = \{1, 5\}$, hence $\varphi(6) = 2$.

TABLE 2. Multiplication table in \mathbb{Z}_{10}^\times .

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$$1^{-1} = 1; 3^{-1} = 7;$$

$$7^{-1} = 3; 9^{-1} = 9.$$

- (Euler's product formula) *If n admits the prime factorization $n = a_1^{r_1} \cdots a_k^{r_k}$, then one has the relation (5) between $\varphi(n)$ and the primes a_i , $i = 1, \dots, k$.*

$$(5) \quad \varphi(n) = n \left(1 - \frac{1}{a_1}\right) \cdots \left(1 - \frac{1}{a_k}\right) = n \prod_{n|a} \left(1 - \frac{1}{a}\right)$$

where the product is over the distinct prime numbers dividing n .

- (Euler's classical formula) *The relation between n , its positive divisors d and the Euler's totient function φ , is given by the formula (6).*

$$(6) \quad \sum_{n|d} \varphi(d) = n.$$

where the sum is over the positive divisors d of n .

- (Euler's theorem) *If a is a generator of \mathbb{Z}_n , then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Lemma 2.3 (The ring \mathbb{Z}_n and its automorphism group). *By considering \mathbb{Z}_n a ring, one has the natural ring isomorphism:*

$$\phi : \mathbb{Z}_n \cong \text{Hom}_{\text{Abelian-group}}(\mathbb{Z}_n, \mathbb{Z}_n),$$

given by $r \mapsto \phi(r)$, $\phi(r)(p) = p^r = \underbrace{p + \cdots + p}_r$. In particular, if r is coprime with n , then $\phi_r : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ is a bijection. Therefore, one has the isomorphism

$$\mathbb{Z}_n^\times \cong \text{Aut}_{\text{Abelian-group}}(\mathbb{Z}_n),$$

where $\mathbb{Z}_n^\times \subset \mathbb{Z}_n$ is the group of units of the ring \mathbb{Z}_n . The elements of \mathbb{Z}_n^\times are the generators of \mathbb{Z}_n .⁸

Lemma 2.4. *Let H be a subgroup of \mathbb{Z}_n , of order b and index c in \mathbb{Z}_n . Then one has $n = bc$ and $H = \frac{c\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_b \cong \frac{\mathbb{Z}}{b\mathbb{Z}}$. The situation is resumed by the exact*

⁸Let us recall that a *unit* for an unital commutative ring R is an element a that admits *inverse*, i.e., an element a^{-1} , such that $aa^{-1} = 1$. If $\text{g.c.d.}(n, a) = 1$ in \mathbb{Z} , then, a identifies in \mathbb{Z}_n an unity. In fact, if a is coprime with n , then holds the following equation in \mathbb{Z} : $x \cdot 2n + y \cdot a = 1$, hence $y \cdot a = 1 - x \cdot 2n$, for some $x, y \in \mathbb{Z}$. This means that we can write $y \cdot a \equiv 1 \pmod{2n}$, or simply $y \cdot a \equiv 1$ in \mathbb{Z}_n . Therefore $y = a^{-1} \in \mathbb{Z}_n^\times \subset \mathbb{Z}_n$. In Tab. 2 is reported the multiplication table of \mathbb{Z}_{10}^\times and in Tab. 3 the multiplication table of \mathbb{Z}_{22}^\times . The group of units of \mathbb{Z} is $\mathbb{Z}^\times = \{-1, +1\}$.

TABLE 3. Multiplication table in \mathbb{Z}_{22}^\times .

	1	3	5	7	9	13	15	17	19	21
1	1	3	5	7	9	13	15	17	19	21
3	3	9	15	21	5	17	1	7	13	19
5	5	15	3	13	1	21	9	19	7	17
7	7	21	13	5	19	3	17	9	1	15
9	9	5	1	19	15	7	3	21	17	13
13	13	17	21	3	7	15	19	1	5	9
15	15	1	9	17	3	19	5	13	21	7
17	17	7	19	9	21	1	13	3	15	5
19	19	13	7	1	17	5	21	15	9	3
21	21	19	17	15	13	9	7	5	3	1

$1^{-1} = 1$; $3^{-1} = 15$; $5^{-1} = 9$; $7^{-1} = 19$; $9^{-1} = 5$;
 $13^{-1} = 17$; $15^{-1} = 3$; $17^{-1} = 13$; $19^{-1} = 7$;
 $21^{-1} = 21$.

commutative diagram (7).

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & n\mathbb{Z} & \longrightarrow & c\mathbb{Z} & \longrightarrow & \boxed{\frac{c\mathbb{Z}}{n\mathbb{Z}} = \frac{c\mathbb{Z}}{bc\mathbb{Z}} \cong \frac{\mathbb{Z}}{b\mathbb{Z}} = \mathbb{Z}_b} \longrightarrow 0 \\
 & & \parallel & & \downarrow & & \downarrow \\
 0 & \longrightarrow & n\mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}_n \longrightarrow 0 \\
 & & & & \downarrow & & \downarrow \\
 & & & & \mathbb{Z}_c & \xlongequal{\quad} & \mathbb{Z}_c \\
 & & & & \downarrow & & \downarrow \\
 & & & & 0 & & 0
 \end{array}$$

- There is a one-to-one correspondence between the ideals $b\mathbb{Z}$ of \mathbb{Z} that contain the ideal $n\mathbb{Z}$ and the ideals of \mathbb{Z}_n : $b\mathbb{Z} = \phi^{-1}(\mathbb{Z}_b)$, with $n|b$.
- For any ideal $n\mathbb{Z} \subset \mathbb{Z}$, $n > 1$, there exists a maximal ideal $m\mathbb{Z} \subset \mathbb{Z}$, containing $n\mathbb{Z}$. More precisely, if n admits the following prime factorization $n = p_1^{r_1} \cdots p_k^{r_k}$, then any maximal ideal $p_i\mathbb{Z}$, $i = 1, \dots, k$, contains $n\mathbb{Z}$.

• Let $r < m$ and p be positive integers, such that $(m - r)|p$, i.e., $m - r = pq$, for some positive integer $q \geq 1$. One has the exact commutative diagram (8).

$$(8) \quad \begin{array}{ccccccc} & & & & 0 & & \\ & & & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_{m-r} & \longrightarrow & \mathbb{Z}_{m-r}/\mathbb{Z}_p \longrightarrow 0 \\ & & & & \downarrow & & \\ & & & & \mathbb{Z}_q & & \\ & & & & \downarrow & & \\ & & & & 0 & & \end{array}$$

• Furthermore iff p and q are coprimes then $\mathbb{Z}_{m-r} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q$.⁹
 • For any couple (m, p) of positive integers, with $p \leq m$, one can find another couple (q, r) of positive integers, such that $\mathbb{Z}_p \subset \mathbb{Z}_{m-r}$ and $\mathbb{Z}_{m-r}/\mathbb{Z}_p \cong \mathbb{Z}_q$.
 In particular if $m = p$, one has $(q, r) = (1, 0)$, hence the following isomorphisms: $\mathbb{Z} = \mathbb{Z}_p \subset \mathbb{Z}_{m-r} = \mathbb{Z}$ and $\mathbb{Z}_q = 0 = \mathbb{Z}_{m-r}/\mathbb{Z}_p = \mathbb{Z}/\mathbb{Z}$.

Lemma 2.5 (Group of units and prime factorization). • If n admits the prime factorization $n = a_1^{r_1} \cdots a_k^{r_k}$, then one has the isomorphism (9).

$$(9) \quad \mathbb{Z}_n^\times \cong \mathbb{Z}_{a_1^{r_1}}^\times \times \cdots \times \mathbb{Z}_{a_k^{r_k}}^\times.$$

• The multiplicative group $\mathbb{Z}_{a^r}^\times$ is cyclic for odd primes a .
 • The multiplicative group \mathbb{Z}_n^\times is cyclic iff $\varphi(n) = \lambda(n)$, where $\lambda(n)$ is the Carmichael function of n , i.e., the least common multiple (l.c.m.) of the order of the cyclic groups in the direct product (9).¹⁰

Proof. It is a consequence of Lemma 1.2(8) and of the fact that under multiplication the congruence classes modulo n which are relatively primes to n satisfy the axioms for an abelian group. \square

Lemma 2.6 (Group of units and primality). A positive integer $m > 1$ is prime iff $\varphi(m) = m - 1$.

Proof. This follows from Euler's product formula (Lemma 5) and according to Lemma 2.5. In fact, m is prime iff $m = a \in P$, hence $|\mathbb{Z}_m^\times| = |\mathbb{Z}_m| - 1 = m - 1$. \square

Lemma 2.7 (Maximal ideals in \mathbb{Z}). In the set Σ of all ideals, $\neq \langle 1 \rangle$, of \mathbb{Z} any chain has at least a maximal ideal.

In particular, any chain in Σ , that ends with a prime ideal $d\mathbb{Z}$, i.e., d is a prime number, has this ideal as maximal ideal.

⁹If $n = p_1^{r_1} \cdots p_k^{r_k}$ is the prime factorization of the integer n , one has the isomorphism $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{r_k}}$. (See also [11].)

¹⁰For example, the group \mathbb{Z}_{10}^\times (see Tab. 2) is cyclic of order 4. In fact, one has the splitting $\mathbb{Z}_{10}^\times \cong \mathbb{Z}_2^\times \oplus \mathbb{Z}_5^\times$. $\varphi(10) = 4$, $\varphi(2) = 1$, $\varphi(5) = 4$ and $\lambda(10) = \text{l.c.m.}(1, 4) = 4$. Thus $\varphi(10) = \lambda(10)$, hence \mathbb{Z}_{10}^\times is cyclic. (For any $a \in \mathbb{Z}_{10}^\times$, one has $a^4 = 1$.) Another example is $\mathbb{Z}_{22}^\times \cong \mathbb{Z}_2^\times \oplus \mathbb{Z}_{11}^\times$, (see Tab. 3), where $\varphi(22) = 10 = \lambda(22) = \text{l.c.m.}(1, 10) = 10$. So the multiplicative group \mathbb{Z}_{22}^\times is cyclic of order 10. (For any element $a \in \mathbb{Z}_{22}^\times$, one has $a^{10} = 1$.)

Proof. Let order Σ by inclusion. Let apply Zorn's lemma to Σ , i.e., let us show that every chain in Σ has an upper bound in Σ . In fact, let $(n_\alpha \mathbb{Z})_{1 \leq \alpha \leq r}$ be a chain of ideals such that $n_i \mathbb{Z} \subseteq n_{i+1} \mathbb{Z}$. Set $\mathfrak{a} = \bigcup_{1 \leq \alpha \leq r} n_\alpha \mathbb{Z}$. Then \mathfrak{a} is an ideal and $1 \notin \mathfrak{a}$ because $1 \notin n_\alpha \mathbb{Z}$ for all α . Hence $\mathfrak{a} \in \Sigma$, and \mathfrak{a} is an upper bound of the chain. From Zorn's lemma Σ must have at least a maximal element. In fact, from Lemma 2.4 it follows that in order to be satisfied the condition on the chain, must be $n_i | n_{i+1}$. On the other hand, since all ideals in \mathbb{Z} are principal, must there exist a positive integer d , such that $\mathfrak{a} = d\mathbb{Z}$. Really if $n_r = p_1^{s_1} \cdots p_k^{s_k}$ is the prime factorization of n_r , we can see that \mathfrak{a} can coincide with any of the following maximal ideals $p_i \mathbb{Z}$, $i = 1, \dots, k$. In particular if $k = 1$, i.e., n_r is a prime number, there exists only one maximal ideal of the chain. \square

Lemma 2.8 (Maximal ideals in \mathbb{Z}_n). *The maximal ideals in \mathbb{Z}_n are $p_i \mathbb{Z}/n\mathbb{Z}$, $i = 1, \dots, k$, if $n = p_1^{r_1} \cdots p_k^{r_k}$ is the prime factorization of n .*

Proof. The proof follows directly from Lemma 2.4 and Lemma 2.7. \square

Lemma 2.9 (Jacobson radical of the ring \mathbb{Z}). *The Jacobson radical $J(\mathbb{Z})$ of \mathbb{Z} , is for definition, the intersection of the maximal ideals of \mathbb{Z} , hence $J(\mathbb{Z}) = \{0\}$. The Jacobson radical of the ring \mathbb{Z}_n is $J(\mathbb{Z}_n) = p_1 \cdots p_k \mathbb{Z}/n\mathbb{Z}$, if $n = p_1^{r_1} \cdots p_k^{r_k}$ is the prime factorization of n . ($J(\mathbb{Z}_n)$ coincides with the nilradical of \mathbb{Z}_n .)¹¹*

- $\mathbb{Z}_n/J(\mathbb{Z}_n)$, is a semiprimitive ring.¹²
- \mathbb{Z}_n , with n prime is a semiprimitive ring, (since it is a field).

Lemma 2.10 (Local rings and semi-local rings). • \mathbb{Z} is not a local ring and neither a semi-local ring.

- \mathbb{Z}_n is a semi-local ring. If n is prime \mathbb{Z}_n becomes a local ring with $\{0\} = J(\mathbb{Z}_n)$ the unique maximal ideal. Therefore $J(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \mathbb{Z}_n^\times = \{0\}$, since \mathbb{Z}_n is a field, hence semiprimitive.

Proof. These are direct consequences of the following definitions and results in commutative algebra. A *local ring* is a ring with exactly one maximal ideal. A *semi-local ring* is a ring with a finite number of maximal ideals. In a local ring R , $J(R) = R \setminus R^\times$, i.e., the Jacobson radical coincides with the non-units of R . In a local ring R , $R/J(R) \cong R/\mathfrak{m}$ is a field, hence semiprimitive. Here \mathfrak{m} is the unique maximal ideal of R . \square

Lemma 2.11 (Nilradical). *The nilradical $\mathfrak{n}(\mathbb{Z})$ of \mathbb{Z} coincides with $J(\mathbb{Z})$: $\mathfrak{n}(\mathbb{Z}) = J(\mathbb{Z}) = \{0\}$.*

The same happens for the ring \mathbb{Z}_n : $\mathfrak{n}(\mathbb{Z}_n) = J(\mathbb{Z}_n)$.

Proof. Let us recall that the nilradical of a ring R is the ideal $\mathfrak{n}(R)$ of its elements $x \in R$, such that $x^n = 0$, for some integer $n > 0$. $\mathfrak{n}(R)$ is obtained by intersection of all prime ideals of R . $\mathfrak{n}(R)$ can be considered the radical of the zero-ideal: $\mathfrak{n}(R) = \mathfrak{r}(< 0 >)$. In general any maximal ideal is prime, but the converse is not true. In fact the ring \mathbb{Z} , has as prime ideals $< m >$, with $m = 0$ or m a prime number $\neq 1$. The maximal ideal are only the ones with m prime, $\neq 1$. However the intersection of all maximal ideals coincides with the ones of all prime ideals and it is just $\{0\}$. Similar considerations hold for the ring \mathbb{Z}_n . \square

¹¹For example $J(\mathbb{Z}_{15}) = \{0\}$. Instead $J(\mathbb{Z}_{12}) = 6\mathbb{Z}/12\mathbb{Z}$.

¹²A semiprimitive ring R is one where $J(R) = \{0\}$. It is always semiprimitive the quotient ring $R/J(R)$, i.e., $J(R/J(R)) = \{0\}$.

Lemma 2.12 (Non-units and maximal ideals). • *Every non-unit of \mathbb{Z} is contained into a maximal ideal.*

• *Every non-unit of \mathbb{Z}_n is contained into a maximal ideal.*

Proof. The proof can be considered as an application of a similar statement for rings. However, let us see a direct proof. Let us start with the ring \mathbb{Z} . Let $n \in \mathbb{Z} \setminus \{-1, 1\}$. Since $n \in n\mathbb{Z} \subseteq p\mathbb{Z}$, where p is any prime such that $n|p$. Therefore n belongs to the maximal ideal $p\mathbb{Z}$.

Let us consider the case of the ring \mathbb{Z}_n . Then if $a \in \mathbb{Z}_n \setminus \mathbb{Z}_n^\times$, it follows that we can write a , considered as belonging to \mathbb{Z}_n , as $a + n\mathbb{Z}$. Since a necessarily divides n , we can write $a = p \cdot q$, for some prime p , such that it appears in the prime factorization of n . Therefore we can write $a = p \cdot q + p \cdot q'\mathbb{Z}$, where $n = p \cdot q'$. As a by product we get $a = p(q + q'\mathbb{Z})$. On the other hand $(p\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/q'\mathbb{Z}) = \mathbb{Z}_{q'}$, and since $p\mathbb{Z}/n\mathbb{Z}$ is a maximal ideal in \mathbb{Z}_n , it follows that belongs to a maximal ideal in \mathbb{Z}_n . As a consequence one has also that $a = p(q + q'\mathbb{Z})$ belongs to the same maximal ideal $\mathbb{Z}_{q'}$ in \mathbb{Z}_n , since $p \cdot q \in \mathbb{Z}_{q'}$. \square

Lemma 2.13 (The rings \mathbb{Z} and \mathbb{Z}_n as \mathbb{Z} -modules). • *The ring \mathbb{Z} has a canonical structure of finitely generated free \mathbb{Z} -module by means of the following short exact sequence:*

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\phi=1} \mathbb{Z} \longrightarrow 0$$

• *The ring \mathbb{Z}_n has a natural structure of finitely generated \mathbb{Z} -module by means of the following short exact sequence:*

$$0 \longrightarrow H_n \longrightarrow \mathbb{Z}^{\varphi(n)} \xrightarrow{\phi} \mathbb{Z}_n \longrightarrow 0$$

where ϕ is defined by

$$x = \phi(x^1, \dots, x^{\varphi(n)}) = \sum_{1 \leq k \leq \varphi(n)} x^k a_k, \quad x^k \in \mathbb{Z}$$

and $\{a_i\}_{1 \leq i \leq \varphi(n)}$ is a set of generators of \mathbb{Z}_n . Furthermore $H_n = \ker(\phi)$, is defined by the linear equation (in \mathbb{Z}_n): $\sum_{1 \leq k \leq \varphi(n)} x^k a_k = 0$. One has the isomorphisms: $\mathbb{Z}_n \cong \mathbb{Z}^{\varphi(n)} / H_n$.

Lemma 2.14 (\mathbb{Z} as a Noetherian ring). • *\mathbb{Z} is a Noetherian ring, i.e., any ascending chain of ideals in \mathbb{Z} , terminates (or stabilizes) after a finite number of steps. The maximal ideal of the chain is a prime ideal, i.e., an ideal of the type $p\mathbb{Z}$ with p a positive prime number.*

• *\mathbb{Z} is not an Artinian ring.*

• (Dimension), $\dim(\mathbb{Z}) = 1$, where $\dim(\mathbb{Z})$ is the supremum of the lengths of chains of prime ideals, in \mathbb{Z} .

• *The prime spectrum $\text{Spec}(\mathbb{Z})$ of \mathbb{Z} is a topological space (with the Zariski topology).*

Proof. In \mathbb{Z} ideals are principal ideals, of the type $m\mathbb{Z} = \langle m \rangle$, where m are positive numbers. Moreover, $m\mathbb{Z} \subseteq n\mathbb{Z}$, iff $m|n$. Therefore, a chain $m\mathbb{Z} \subseteq n\mathbb{Z} \subseteq p\mathbb{Z} \subseteq \dots$, must necessarily terminates after a finite number of steps, since the possible positive numbers that divide m cannot exceed m . Furthermore, taking into account the prime factorization of m it is clear that the maximal ideal in the chain is a prime ideal.

In \mathbb{Z} any descending chain of ideals is of the type

$$m\mathbb{Z} \supseteq p_1 m\mathbb{Z} \supseteq p_2 p_1 m\mathbb{Z} \supseteq \cdots$$

where m, p_i are positive numbers > 1 . Such chains cannot stabilize after a finite number of steps, since we can always find ideals $k\mathbb{Z}$, with k a multiple of the previous one in the chain. The intersection of all such ideals is the trivial ideal $\langle 0 \rangle$.

The strictly increasing chains of prime ideals in \mathbb{Z} are of the type $\mathfrak{p}_0 = \langle 0 \rangle \subset \mathfrak{p}_1 = p\mathbb{Z}$, or $\mathfrak{p}_0 = p\mathbb{Z}$, with $p > 1$ prime. Therefore, the supremum of the lengths of such chains is 1. This is also the dimension of \mathbb{Z} .

The set $\text{Spec}(\mathbb{Z})$ of all prime ideals in \mathbb{Z} is a topological space with Zariski topology, i.e., generated by closed subsets, defined by $V(X)$, for any subset $X \subset \mathbb{Z}$, as the set of all prime ideals of \mathbb{Z} that contain X . $V(X)$ satisfy the following properties.

- (i) If $\mathfrak{a} = \langle X \rangle \subset \mathbb{Z}$, is the ideal generated by X , then $V(X) = V(\mathfrak{a}) = V(\mathfrak{r}(\mathfrak{a}))$. (If $a \in \mathbb{Z}$, then $\mathfrak{a} = a\mathbb{Z}$.)
- (ii) $V(0) = \text{Spec}(\mathbb{Z})$.
- (iii) $V(1) = \emptyset$.
- (iv) If $(X_i)_{i \in I}$ is any family of subsets of \mathbb{Z} , then $V(\bigcup_{i \in I} X_i) = \bigcap_{i \in I} V(X_i)$.
- (v) $V(m\mathbb{Z} \cap n\mathbb{Z}) = V(mn\mathbb{Z}) = V(m\mathbb{Z}) \cup V(n\mathbb{Z})$, for any ideal $m\mathbb{Z}$ and $n\mathbb{Z}$ of \mathbb{Z} .
- (vi) $V(\sum_i \mathfrak{a}_i) = \bigcap_i V(\mathfrak{a}_i)$. The *basic open sets* of $\text{Spec}(\mathbb{Z})$ is made by sets $X_a = \text{Spec}(\mathbb{Z}) \setminus V(a)$, for any $a \in \text{Spec}(\mathbb{Z})$. The sets X_a are open sets in the Zariski topology of $\text{Spec}(\mathbb{Z})$, and satisfy to the following properties.
- (vii) $X_a \cap X_b = X_{ab}$.
- (viii) $X_a = \emptyset \Leftrightarrow a$ is nilpotent.
- (ix) $X_a = \text{Spec}(\mathbb{Z}) \Leftrightarrow a$ is a unit.
- (x) $X_a = X_b \Leftrightarrow \mathfrak{r}(\langle a \rangle) = \mathfrak{r}(\langle b \rangle)$.
- (xi) $\text{Spec}(\mathbb{Z})$ is quasi-compact (that is, every open covering of $\text{Spec}(\mathbb{Z})$ has a finite subcovering).¹³
- (xii) Each X_a is quasi-compact.
- (xiii) An open subset of $\text{Spec}(\mathbb{Z})$ is quasi-compact iff it is a finite union of sets X_a .
- (xiv) Let $\langle x \rangle \in \text{Spec}(\mathbb{Z})$, be a point of the prime spectrum of \mathbb{Z} , i.e., x prime. Then $\langle x \rangle \equiv x\mathbb{Z}$ is closed in the Zariski topology of \mathbb{Z} iff $x\mathbb{Z}$ is maximal. On the other hand all prime ideals in \mathbb{Z} are maximal ones, hence any point $\langle x \rangle$ is closed in $\text{Spec}(\mathbb{Z})$. Therefore, $\text{Spec}(\mathbb{Z})$ is a T_0 -space, i.e., if $\langle x \rangle$ and $\langle y \rangle$ are distinct points of $\text{Spec}(\mathbb{Z})$, then either there is a neighborhood of $\langle x \rangle$ which does not contain $\langle y \rangle$, or else there is a neighborhood of $\langle y \rangle$ which does not contain $\langle x \rangle$.
- (xv) $\text{Spec}(\mathbb{Z})$ is an *irreducible space*, i.e., any pair of non-empty open sets in the Zariski topology, intersect, or equivalently every non-empty open set is dense in $\text{Spec}(\mathbb{Z})$. This is equivalent to say that $\mathfrak{n}(\mathbb{Z}) = \langle 0 \rangle$.
- (xvi) $\text{Spec}(\mathbb{Z}) = \{\mathfrak{p} \mid \mathfrak{p} \subset \mathbb{Z} \text{ primeideal}\} \cup \{\langle 0 \rangle\}$. Every prime ideal is closed in $\text{Spec}(\mathbb{Z})$, except $\langle 0 \rangle$, whose closure is $V(0) = \text{Spec}(\mathbb{Z})$. \square

Lemma 2.15 (\mathbb{Z}_n as a Noetherian and Artinian ring). • \mathbb{Z}_n is a Noetherian and Artinian ring.

¹³"Quasi-compact" means "compact but not necessarily Hausdorff".

Proof. Since \mathbb{Z}_n is a finitely generated commutative ring, it is a Noetherian ring.¹⁴ More precisely, any ascending chain of ideals in \mathbb{Z}_n is of the type:

$$p\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_q \subseteq r\mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}_s \subseteq \dots$$

where $n = pq$, $q = rs$, etc. This chain necessarily stops after a finite number of steps since the numbers q , r , etc. all divide n , hence the steps in the chain cannot be more than n . Furthermore, the last ideal in the chain must be corresponding to a prime number, that results a maximal ideal.

To prove that \mathbb{Z}_n is Artinian, it is enough to prove that $\dim(\mathbb{Z}_n) = 0$. In fact, any Noetherian ring is an Artinian ring iff its dimension is zero. [1] On the other hand all the prime ideals of \mathbb{Z}_n are of the type \mathbb{Z}_p , where p is a prime number such that $n|p$. Therefore, any strictly increasing chain of prime ideals in \mathbb{Z}_n can be made by only one ideal: $\mathfrak{p}_0 = \mathbb{Z}_p$ with p a prime number, $n|p$, hence the dimension of the ring \mathbb{Z}_n must necessarily be 0. Therefore, \mathbb{Z}_n is an Artinian ring.

This means that any descending chain of ideals in \mathbb{Z}_n

$$\mathfrak{p}_0 \supseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \dots$$

stops (or stabilizes) after a finite number of steps. Now, after above considerations it results that any ascending chain of ideals in \mathbb{Z}_n is of the type

$$\mathbb{Z}_a \supseteq \mathbb{Z}_b \supseteq \mathbb{Z}_c \supseteq \dots$$

with $a = pb$, $b = rc$, etc. Therefore, since a must be a multiple of any of the numbers b , c etc., it follows that such a chain must stop after a finite number of steps, since a is a fixed number. More precisely, the chain stabilizes at an ideal \mathbb{Z}_x , where x is a prime number entering in the prime factorization of a . \square

Remark 2.16. *Let us emphasize that after Lemma 2.2 one can understand that the numbers $p_1^{(s)}$ and $p_2^{(s)}$ considered in our criterion to find a solution to the Goldbach's conjecture, are just generators of \mathbb{Z}_{2n} . However, they are, in a sense, distinguished generators since they are not only prime with respect to $2n$, but are just prime numbers.*

Definition 2.17 (Strong generators in \mathbb{Z}_m). *We call strong generators in \mathbb{Z}_m the generators that are identified by prime numbers. Let us denote by $\mathbb{Z}_m^\blacksquare$ the set of strong generators of \mathbb{Z}_m . One has the natural inclusions:*

$$\mathbb{Z}_m^\blacksquare \subset \mathbb{Z}_m^\times \subset \mathbb{Z}_m.$$

Proposition 2.18 (Existence of strong generators in a cyclic group). *In \mathbb{Z}_{2n} , $n \geq 1$, there exist strong generators. When $n > 1$, $\mathbb{Z}_{2n}^\blacksquare \supset \{1\}$.*

Proof. In fact in the set of generators of \mathbb{Z}_{2n} there exists always 1, for any positive number $n \geq 1$. However, when $n > 1$, $\mathbb{Z}_{2n}^\blacksquare$ properly contains 1. Let us denote respectively by p_k the primes entering in the factorization of $2n$, a_i the units that are not primes and by b_j the units that are primes. The prime factorization of a_k must be of the type $a_k = b_1^{m_1} \dots b_h^{m_h}$, since a_k are coprimes with $2n$. Then any $c \in \mathbb{Z}_{2n}$ can be written in the form $c = x^k a_k + y^j b_j$, $x^k, y^j \in \mathbb{Z}$. If we assume that with $n > 1$, $\mathbb{Z}_{2n}^\blacksquare = \{1\}$, then also the units a_k should reduce to 1, and any $c \in \mathbb{Z}_{2n}$, should be written $c = x \cdot 1$. This can be happen iff $\mathbb{Z}_{2n} = \mathbb{Z}_2$, hence $n = 1$, in

¹⁴Another, way to prove that \mathbb{Z}_n is a Noetherian ring, is to use the following theorem: If R is a Noetherian ring, and \mathfrak{a} is an ideal of R , then R/\mathfrak{a} is a Noetherian ring too.[1] In fact, it is enough to take $R = \mathbb{Z}$ and $\mathfrak{a} = n\mathbb{Z}$. This agrees with the epimorphism $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_n$, since $\mathbb{Z}_n \cong \mathbb{Z}/\ker(\pi)$.

TABLE 4. Examples of strong generators in \mathbb{Z}_{2n} .

\mathbb{Z}_{2n}	Goldbach's couples (\clubsuit)	\mathbb{Z}_{2n}^\times (Generators group or group of units)	$\varphi(2n)$	Quasi-Goldbach's couples (\spadesuit)
\mathbb{Z}_2	(1, 1) *	{1}	1	—
\mathbb{Z}_4	(1, 3) *	{1, 3}	2	—
\mathbb{Z}_6	(1, 5) *	{1, 5}	2	—
\mathbb{Z}_8	(1, 7) * ; (3, 5)	{1, 3, 5, 7}	4	—
\mathbb{Z}_{10}	(3, 7) *	{1, 3, 7, (9)}	4	(1, 9)
\mathbb{Z}_{12}	(1, 11) * ; (5, 7)	{1, 5, 7, 11}	4	—
\mathbb{Z}_{14}	(1, 13) * ; (3, 11)	{1, 3, 5, (9), 11, 13}	6	(5, 9)
\mathbb{Z}_{16}	(3, 13) * ; (5, 11)	{1, 3, 5, 7, (9), 11, 13, (15)}	8	(1, 15); (7, 9)
\mathbb{Z}_{18}	(1, 17) * ; (5, 13); (7, 11)	{1, 5, 7, 11, 13, 17}	6	—
\mathbb{Z}_{20}	(1, 19) * ; (3, 17); (7, 13)	{1, 3, 7, (9), 11, 13, 17, 19}	8	(9, 11)
\mathbb{Z}_{22}	(3, 19) * ; (5, 17)	{1, 3, 5, 7, (9), 11, 13, (15), 17, 19, 21}	10	(1, 21); (7, 15); (9, 13)
\mathbb{Z}_{28}	(5, 23) * ; (11, 17)	{1, 3, 5, (9), 11, 13, (15), 17, 19, 23, (25), (27)}	12	(1, 27); (3, 25); (9, 19); (13, 15)

The Goldbach's couples marked by (\star) are ones obtained by criterion in Tab. 1.

The set of strong generators is obtained by the ones of generators, by forgetting the numbers between brackets () in \mathbb{Z}_{2n}^\times .

$\mathbb{Z}_{2n}^\times = \{k \in \mathbb{Z}_{2n} \mid g.c.d.(2n, k) = 1, 1 \leq k < 2n\}$ is also called the *multiplicative group of integers (mod 2n)*.

(\clubsuit) Warn ! In this table, except for the case $n = 1$, do not appear *trivial Goldbach couples*, $((n, n))$ with n prime.

(\spadesuit) Except in the case $n = 1$, trivial Goldbach couples are never identified by units in \mathbb{Z}_{2n} . (See Lemma 2.23.)

(\spadesuit) In this table are reported the quasi-Goldbach couples that are not Goldbach couples.

contrast with the assumption that $n > 1$. This just means that for $n > 1$, $\mathbb{Z}_{2n}^\blacksquare$ is larger than $\{1\}$. \square

Example 2.19. In Tab. 4 we report generators and strong generators, with respect to examples just considered in Tab. 1. There we can verify that some couples of generators satisfy equation $2n = a + b$, but these do not necessitate to be strong generators in \mathbb{Z}_{2n} .

So, in order to prove GC, we are conduced to prove Theorem 2.20.

Theorem 2.20 (Goldbach's couples in \mathbb{Z}_{2n}). \bullet In the group \mathbb{Z}_{2n} there exist two strong generators identified by positive primes a and b that satisfy the condition (10).

$$(10) \quad 2n = a + b, \quad a, b \in P.$$

- We call Goldbach's couples in \mathbb{Z}_{2n} , couples of strong generators of \mathbb{Z}_{2n} , identified by two positive primes a and b that satisfy the condition (10).¹⁵
- We call also quasi-Goldbach's couples in \mathbb{Z}_{2n} , couples of generators (a, b) of \mathbb{Z}_{2n} , that satisfy the condition $2n = a + b$, but where one of the numbers a or b does not necessitate to be prime. (All Goldbach couples are also quasi-Goldbach couples.)
- Goldbach's couples do not necessitate to be unique in \mathbb{Z}_{2n} , for any $n > 3$.
- We call canonical Goldbach couple of $2n$, the first obtained by applying the criterion in Tab. 1.
- We call Noether-Goldbach's couple in \mathbb{Z}_{2n} , the quasi-Goldbach couple $(1, 2n - 1)$, when it is also a Goldbach couple. If there exists the Noether-Goldbach couple, this is the canonical one too.

Proof. Let us consider the following lemmas.

Lemma 2.21. The strong generators of \mathbb{Z}_{2n} satisfy the following properties.

- (i) Each strong generator of \mathbb{Z}_{2n} , generates all \mathbb{Z}_{2n} .

¹⁵In the following we shall often use the same symbol to denote a number $a \in \mathbb{Z}$ and its projection $\pi(a) \in \mathbb{Z}_m$, via the canonical projection $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_m$. In fact, from the context it will be clear what is the right interpretation !

(ii) If $p_1 \in \mathbb{Z}_m^\blacksquare$ then $2n - p_1 = p_2$ is a generator of \mathbb{Z}_{2n} , i.e., $p_2 \in \mathbb{Z}_{2n}^\times$. Then p_2 has the prime factorization (11).

$$(11) \quad p_2 = b_1^{u_1} \cdots b_s^{u_s}$$

where b_i identify strong generators in \mathbb{Z}_{2n} . Therefore p_2 is coprime with p_1 iff $b_i \neq p_1$, $i = 1, \dots, s$.

Proof. The first proposition follows from the fact that a strong generator is a unit of \mathbb{Z}_{2n} .

The second proposition follows from the prime factorization of $2n = a_1^{r_1} \cdots a_k^{r_k}$. In fact these primes numbers cannot coincide with p_1 , since this last is a unit, hence $\text{g.c.d.}(2n, p_1) = 1$. Therefore the number $2n - p_1 = p_2$ cannot be factorized as $a_s^m q$, with a_s coinciding with a prime number a_i , appearing in the prime factorization of $2n$. In other words $\text{g.c.d.}(2n, p_2) = 1$, hence $p_2 \in \mathbb{Z}_{2n}^\times$. Furthermore, if $p_2 \in \mathbb{Z}_{2n}^\times$ then in its prime factorization $p_2 = b_1^{u_1} \cdots b_s^{u_s}$ cannot appear the prime numbers of the prime factorization of $2n = a_1^{r_1} \cdots a_k^{r_k}$. This proves the factorization (11), hence the condition in order p_2 should be coprime with p_1 . \square

Lemma 2.22. Let $p_2 \in \mathbb{Z}_{2n}^\times \subset \mathbb{Z}_{2n}$, as defined in Lemma 2.21. p_2 is prime iff it identifies a strong generator in \mathbb{Z}_{2n} , i.e., p_2 (or more precisely its projection in \mathbb{Z}_{2n}) belongs to $\mathbb{Z}_{2n}^\blacksquare \subset \mathbb{Z}_{2n}^\times \subset \mathbb{Z}_{2n}$.

Proof. This follows directly from prime factorization (11). \square

Lemma 2.23 (Existence of trivial Goldbach couples). If $2n$ admits the prime factorization $2n = a_1^{r_1} \cdots a_k^{r_k}$, then one has $2n - a_i \in P[1, 2n]$ iff $2n = 2a_i$. Here $P[1, 2n]$ denotes the set of primes in the interval $[1, 2n]$. Thus, except in the trivial cases, i.e., where n is a prime a_i , to the primes $a_i \in P[1, 2n]$, entering in the prime factorization of $2n$, cannot be associated Goldbach couples of $2n$. Therefore, in non-trivial cases, a necessary condition for the Goldbach couples (p_1, p_2) of $2n$ is that $p_2 = 2n - b$, with b identifying in \mathbb{Z}_{2n} strong generators, namely $b \in \mathbb{Z}_{2n}^\blacksquare$.

Proof. Let us note that in $P[1, 2n]$ admits the following partition in two disjoint sets: $P[1, 2n] = P[1, 2n]^\square \sqcup P[1, 2n]^\blacksquare$, where $P[1, 2n]^\square$ denotes the primes entering in the factorization of $2n$ and $P[1, 2n]^\blacksquare$ are the other primes that identify strong generators in \mathbb{Z}_{2n} . If we denotes by $\mathbf{P}[1, 2n]$ the projection of $P[1, 2n]$ into \mathbb{Z}_{2n} , by means of the canonical epimorphism $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_{2n}$, then we induce the following partition in $\mathbf{P}[1, 2n]$: $\mathbf{P}[1, 2n] = \mathbb{Z}_{2n}^\square \sqcup \mathbb{Z}_{2n}^\blacksquare$, where $\mathbb{Z}_{2n}^\square = \pi(P[1, 2n]^\square) \subset \mathbb{Z}_{2n}$. In order to see under which conditions $2n - a_i$ is prime, let us represent this number with respect the prime factorization of $2n$.

$$(12) \quad \begin{cases} 2n - a_i &= a_1^{r_1} \cdots a_k^{r_k} - a_i \\ &= a_i(a_1^{r_1} \cdots a_i^{r_i-1} \cdots a_k^{r_k} - 1) \end{cases}$$

Therefore, $2n - a_i$ is prime iff $a_1^{r_1} \cdots a_i^{r_i-1} \cdots a_k^{r_k} - 1 = 1$, namely $a_1^{r_1} \cdots a_i^{r_i-1} \cdots a_k^{r_k} = 2$. This condition can be verified iff $2n = 2a_i$. \square

Lemma 2.24 (Maximal ideals and $2n - 1$). • If $2n$ admits the prime factorization $2n = a_1^{r_1} \cdots a_k^{r_k}$, $a_i \in P[1, 2n]$, then $2n - 1$ cannot belong to the ideal $\mathbb{Z}_{a_i} \subset \mathbb{Z}_{2n}$.

• The same holds for any element of \mathbb{Z}_{2n}^\times .

• Any element of \mathbb{Z}_{2n}^\times cannot belong to the Jacobson radical $J(\mathbb{Z}_{2n}) \cong a_1 \cdots a_k \mathbb{Z} / 2n \mathbb{Z}$, namely the intersection of all maximal ideals of \mathbb{Z}_{2n} .

Proof. In fact $2n - 1$ is coprime with $2n$, hence identifies an element of \mathbb{Z}_{2n}^\times . Therefore, it cannot be contained into a maximal ideal of \mathbb{Z}_{2n} . These are of the type \mathbb{Z}_{a_i} , where a_i is a prime entering in the prime factorization of $2n$.

The other propositions are direct consequences of above properties. \square

Lemma 2.25 (Mirror symmetry in \mathbb{Z}_{2n}^\times). *The integers a_i in the interval $[1, 2n]$, that identify units in \mathbb{Z}_{2n} , are symmetrically distributed around the middle. Therefore, in \mathbb{Z}_{2n}^\times the order is always even: $\varphi(2n) = 2d$.¹⁶*

Proof. In fact, from any of such a_i we can see that $2n - a_i = a_j$ where a_j identifies another unit in \mathbb{Z}_{2n} . The proof is similar to the one considered for the Lemma 2.21. \square

Lemma 2.26 (Mirror symmetry in Goldbach couples and existence of Goldbach couples and Noether-Goldbach couples). *• For any fixed even integer $2n$, $n \geq 1$, the Goldbach couples are symmetrically distributed around the middle in the interval $[1, 2n]$.*

- Goldbach couples are identified by $b_i \in \mathbb{Z}_{2n}^\square$, $b_i \geq n$ iff there exists a strong generator b_j , symmetric to b_i with respect to the middle, or equivalently $b_i - n = n - b_j$.
- In the case that $b_i = n$, then there exists the trivial Goldbach couple (n, n) .
- The Noether-Goldbach couple of $2n$, $n > 1$, exists iff the order of \mathbb{Z}_{2n-1}^\times is $2(n-1)$.

Proof. In fact, for any Goldbach couple (p_1, p_2) we can write the condition $2n = p_1 + p_2$ in the form $p_1 - n = n - p_2$.

The second proposition follows directly from the previous one.

If $2n-1$ is a prime, then the quasi-Goldbach couple $(2n-1, 1)$ becomes a (canonical) Noether-Golbach couple. On the other and a positive integer m is prime iff the order of \mathbb{Z}_m^\times is $m-1$, i.e. $\varphi(m) = m-1$. (Lemma 2.6.) Therefore $2n-1$ is prime iff the order of \mathbb{Z}_{2n-1}^\times is $2n-1-1 = 2(n-1)$. \square

Even if there is a mirror symmetry in the distribution of the Goldbach-couples, this does not origin from an analogous symmetry in the set of strong generators. In fact, we get the following lemma.

Lemma 2.27 (No-mirror symmetry in \mathbb{Z}_{2n}^\square). *The strong generators do not respect the mirror symmetry, in the sense that if there exists a strong generator $b_i \geq n$ of $2n$, does not necessitate that there is also a strong generator $b_j \leq n$, such that $b_i - n = n - b_j$.*

Proof. This can be proved with a counterexample. For example in \mathbb{Z}_{10} , the mirror symmetric of 1 does not exist. This should be 9, but it is not prime. Another example could be 556, where the strong generator 547 has not a mirror symmetric strong generator. (See Tab. 1.) In fact, the absence of mirror symmetry in \mathbb{Z}_{2n}^\square produces quasi-Goldbach couples that are not Goldbach couples. \square

Definition 2.28 (Noether numbers). *We call Noether numbers the even numbers $2n$ such in \mathbb{Z}_{2n} there exists a (canonical) Noether-Goldbach couple.*

Lemma 2.29 (Existence of Noether-numbers). *$2n$ is a Noether number iff the order of \mathbb{Z}_{2n-1}^\times is $2(n-1)$.*

Proof. This is a by-product of Lemma 2.26 and Definition 2.28 \square

¹⁶See Tab. 4 for some examples.

Lemma 2.30 (Goldbach couples, splitting of the ring \mathbb{Z} and algebraic relations in \mathbb{Z} and \mathbb{Z}_{2n}). • Any non-trivial Goldbach couple (b_i, b_j) , $i \neq j$, $b_i, b_j \in \mathbb{Z}_{2n}^\blacksquare$, gives split representation of the ring \mathbb{Z} : $\mathbb{Z} = b_i\mathbb{Z} + b_j\mathbb{Z}$.

This means that hold the equations (13) relating the elements in a same Goldbach couple, but also different elements of different Goldbach couples, and with $2n$.

$$(13) \quad \left\{ \begin{array}{l} b_i \cdot x + b_j \cdot y = 1, i \neq j, x, y \in \mathbb{Z} \\ 2n \cdot \bar{x} + b \cdot \bar{y} = 1, i \neq j, \bar{x}, \bar{y} \in \mathbb{Z} \end{array} \right\} b_i, b_j, b \in P[1, 2n]^\blacksquare$$

Above equations (13) can be reinterpreted as equations in \mathbb{Z}_{2n} .

Proof. In fact, it is enough to apply Lemma 1.2, taking into account that $2n$ is coprime with any $b \in P[1, 2n]^\blacksquare$. Furthermore equations (13) can be reinterpreted in \mathbb{Z}_{2n} , taking into account the isomorphisms (14).

$$(14) \quad \left\{ \begin{array}{l} (b_i\mathbb{Z} + b_j\mathbb{Z})/2n\mathbb{Z} \cong \mathbb{Z}/2n\mathbb{Z} = \mathbb{Z}_{2n} \\ (2n\mathbb{Z} + b\mathbb{Z})/2n\mathbb{Z} \cong \mathbb{Z}/2n\mathbb{Z} = \mathbb{Z}_{2n} \end{array} \right.$$

□

Example 2.31. Let us consider the case $2n = 22$. See Tab. 4 for corresponding characterizations of Goldbach couples. Then $p_2 = 2n - 1 = 21$ is not a prime number, in other word $(1, 21)$ is a quasi Goldbach couple. (In fact the canonical Goldbach couple is $(3, 19)$.) However, the equation $22 - 21 = 1$ says that 22 is coprime with 21, hence this equation written in \mathbb{Z} , can be rewritten also in \mathbb{Z}_{22} , where we can write $19 \cdot 19^{-1} = 1$. (See Tab. 3.) In this way we get the following equation in \mathbb{Z}_{22} . $22 \cdot 21 - 19 \cdot 15 = 1$. This can be rewritten in \mathbb{Z} , since 21 and 19 are coprimes. We get $-9 \cdot 21 + 10 \cdot 19 = 1$. Instead if we made a similar calculation with $3 \cdot 3^{-1} = 1$ in \mathbb{Z}_{22} we arrive to the following equation $x21 + y3 = 1$, with $x = 22$ and $y = -21 \cdot 3^{-1}$. This equation cannot be rewritten in \mathbb{Z} , since 21 is not coprime with 3.

Lemma 2.32 (Strong generators and ring isomorphisms). Let $\{b_j\}_{1 \leq j \leq s}$ be the strong generators of \mathbb{Z}_{2n} . Then one has the ring isomorphism

$$(15) \quad \mathbb{Z}_{b_1 \dots b_s} \cong \prod_j \mathbb{Z}_{b_j}.$$

Proof. In fact one has the short exact sequence (16).

$$(16) \quad 0 \longrightarrow \boxed{\ker(\phi) = \bigcap_j b_j\mathbb{Z}} \longrightarrow \mathbb{Z} \xrightarrow{\phi} \prod_j (\mathbb{Z}/b_j\mathbb{Z}) \longrightarrow 0$$

The morphism ϕ is surjective since the ideals $b_j\mathbb{Z} \subset \mathbb{Z}$ are primes. Therefore one has the isomorphism

$$\mathbb{Z}/\ker(\phi) \cong \mathbb{Z}/b_1 \dots b_s\mathbb{Z} = \mathbb{Z}_{b_1 \dots b_s} \cong \prod_j (\mathbb{Z}_{b_j}).$$

□

From above lemmas, and taking into account the criterion in Tab. 1, it is clear that since the set $\mathbb{Z}_{2n}^\blacksquare$ is finite, and contains prime numbers, even if these do not respect the mirror-symmetry with respect to the middle of the interval $[1, 2n]$, (see Proposition 2.18, Lemma 2.26 and Lemma 2.27), it follows that $p_2 + a = 2n - (p_1 - a)$ must necessarily coincide with a prime number after some finite steps. In fact, in each of this step $p_1 - a \geq n$ is taken a strong generator. More precisely, if \mathbb{Z}_{2n-1}^\times

is of order $2(n-1)$, then $2n$ is a Noether number, hence there is the canonical Noether-Goldbach couple $(1, 2n-1)$ of $2n$. Moreover if n is prime, there exists the trivial Goldbach couple (n, n) . Other Goldbach couples, when occur, can be found by considering the $2n - b_j$, with $1 < b_j < 2n - 1$, strong generators in $\mathbb{Z}_{2n}^\blacksquare$. In order to be more explicit in our proof, let us associate to any number $1 < 2n - b_i = a_j < 2n - 1$ in our process, the ideal $\mathfrak{a}_i = (2n - b_i)\mathbb{Z}/r\mathbb{Z} \subset \mathbb{Z}_r$, where $r = \text{l.c.m.}(a_1, \dots, a_k)$. Here we denote by a_i the integers in the open interval $]1, 2n - 1[$ that identify the units of \mathbb{Z}_{2n} , and by b_j , the a_i that are primes, hence their projections under $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_{2n}$, identify the strong generators of \mathbb{Z}_{2n} . Then the set $\{\mathfrak{a}_i\}$ of ideals in \mathbb{Z}_r , associated to the criterion in Tab. 1, must have maximal elements, since \mathbb{Z}_r is Noetherian. (See Lemma 2.15.) Warn ! We are not interested to a maximal ideal of the set $\{\mathfrak{a}_i\}$, but to ideals in $\{\mathfrak{a}_i\}$ that are maximal ideals of \mathbb{Z}_r ! These exist just for the Noetherian structure of the ring \mathbb{Z}_r , and are in a finite number since \mathbb{Z}_r is an Artinian ring. (See Lemma 2.15.) On the other hand, any maximal ideal \mathfrak{m} in \mathbb{Z}_r is of the type $\mathfrak{m} = b\mathbb{Z}/r\mathbb{Z}$, with $b \neq 1$ a prime of the interval $[1, 2n]$, identifying a strong generator of $\mathbb{Z}_{2n}^\blacksquare$. By looking to maximal ideals of \mathbb{Z}_r , in the set $\{\mathfrak{a}_i\}$, we are sure that these are of the type $b\mathbb{Z}/r\mathbb{Z}$, with b some prime $b = 2n - b_i \neq 1$.¹⁷

Lemma 2.33 (Relation between \mathbb{Z}_r and maximal ideals). *Let us denote $\mathfrak{m}_j = \frac{b_j\mathbb{Z}}{r\mathbb{Z}}$, $1 \leq j \leq s$ be the maximal ideals in \mathbb{Z}_r . One has the short exact sequence (17).*

$$(17) \quad 0 \longrightarrow \boxed{\ker(\phi) = \bigcap_j \mathfrak{m}_j} \longrightarrow \mathbb{Z}_r \xrightarrow{\phi} \prod_j (\mathbb{Z}/\mathfrak{m}_j) \longrightarrow 0$$

and therefore one has the following isomorphisms: $\mathbb{Z}_r/\mathfrak{m}_j \cong \mathbb{Z}_{b_j}$, and

$$\mathbb{Z}_r/\ker(\phi) \cong \mathbb{Z}_{b_1 \dots b_s} \cong \prod_j \mathbb{Z}/\mathfrak{m}_j \cong \prod_j \mathbb{Z}_{b_j}.$$

Proof. The proof is similar to the one of Lemma 2.32. \square

Lemma 2.34. *Any two maximal ideals $\mathfrak{m}_1, \mathfrak{m}_2$ in \mathbb{Z}_r are coprimes, i.e., $\mathfrak{m}_1 + \mathfrak{m}_2 = \mathbb{Z}_r$.*¹⁸

Proof. In fact, $\mathfrak{m}_1 + \mathfrak{m}_2 = \frac{b_1\mathbb{Z}}{r\mathbb{Z}} + \frac{b_2\mathbb{Z}}{r\mathbb{Z}} = \frac{b_1\mathbb{Z} + b_2\mathbb{Z}}{r\mathbb{Z}} = \frac{\text{g.c.d.}(b_1, b_2)\mathbb{Z}}{r\mathbb{Z}} = \frac{\mathbb{Z}}{r\mathbb{Z}} = \mathbb{Z}_r$. \square

Lemma 2.35 (Representation of \mathbb{Z}_r by means of local rings). *\mathbb{Z}_r is isomorphic to the direct product of a finite number of local artin rings. Furthermore, one has the canonical isomorphism (18).*

$$(18) \quad \mathbb{Z}_r \cong \prod_{x \in \text{Spec}(\mathbb{Z}_r)} (\mathbb{Z}_r)_x$$

where $(\mathbb{Z}_r)_x$ is \mathbb{Z}_r localized at x .

Proof. In fact, \mathbb{Z}_r is an Artinian ring. (See also Lemma 2.4 and Lemma 2.15.) Furthermore, \mathbb{Z}_r as an Artinian ring, has a finite number of maximal ideals, and in \mathbb{Z}_r all prime ideals are maximal ideals too. (This agrees with the fact that in

¹⁷Warn ! In general \mathbb{Z}_r contains a finite number of maximal ideals, since it is a semi-local ring. (See Lemma 2.10.) Thus, we can identify by means of such maximal ideals all the possible Goldbach couples, when they occur in $\{\mathfrak{a}_i\}$. However, two different maximal ideals can identify the same Goldbach couple for effect of the mirror symmetry. (See Lemma 2.26.)

¹⁸Warn ! Do not confuse the sum with the direct sum. See Lemma 2.38.

Artinian rings all the prime ideals are maximal ones.) Thus $\text{Spec}(\mathbb{Z}_r) = \text{Max}(\mathbb{Z}_r)$. i.e., the prime spectrum coincides with the maximal spectrum. Taking into account that \mathbb{Z}_r is also a Noetherian ring, one has that $\text{Spec}(\mathbb{Z}_r)$ is a finite Hausdorff reducible Noetherian topological space consisting of a finite number of points. These points are closed and open in the Zariski topology, i.e., $\text{Spec}(\mathbb{Z}_r)$ is a discrete topological space. One has the short exact sequence (19).¹⁹

$$(19) \quad 0 \longrightarrow \boxed{\mathbb{Z}_r = \Gamma(\text{Spec}(\mathbb{Z}_r), \mathcal{O}_{\text{Spec}(\mathbb{Z}_r)})} \xrightarrow{\phi} \boxed{\prod_{x \in \text{Spec}(\mathbb{Z}_r)} (\mathbb{Z}_r)_x = \prod_{x \in \text{Spec}(\mathbb{Z}_r)} \mathcal{O}_{\text{Spec}(\mathbb{Z}_r), x}} \longrightarrow 0$$

In fact ϕ is naturally injective. Furthermore, since each point x is also open, then $(\mathbb{Z}_r)_x = \Gamma(\{x\}, \mathcal{O}_{\text{Spec}(\mathbb{Z}_r)})$, and $\{x\} \cap \{y\} = \emptyset$ if $x \neq y$. As a by product, it follows that a section $s \in \Gamma(\text{Spec}(\mathbb{Z}_r), \mathcal{O}_{\text{Spec}(\mathbb{Z}_r)})$ can be built by a collection of sections $s(x) \in \Gamma(\{x\}, \mathcal{O}_{\text{Spec}(\mathbb{Z}_r)})$, for $x \in \text{Spec}(\mathbb{Z}_r)$. Therefore ϕ is surjective too. \square

Lemma 2.36 (Spectral properties of \mathbb{Z}_r and existence of Goldbach couples). *The points $\mathfrak{b}_j = \frac{b_j \mathbb{Z}}{r \mathbb{Z}}$ in $\text{Spec}(\mathbb{Z}_r)$, with $b_j \neq 1$, identifying strong generators in \mathbb{Z}_{2n} , are not accumulation points for the ideals $\mathfrak{a}_i = \frac{(2n-b_i)\mathbb{Z}}{r \mathbb{Z}}$, when $(2n-b_i) = a_i$ is not prime.²⁰*

Proof. In fact, each point $\mathfrak{b}_j \in \text{Spec}(\mathbb{Z}_r)$ has all the neighborhoods of the type $U = \text{Spec}(\mathbb{Z}_r) \setminus \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \in \text{Spec}(\mathbb{Z}_r)$. Then if \mathfrak{a}_i is not a maximal ideal it must be contained in some intersection of maximal ideals of $\text{Spec}(\mathbb{Z}_r)$, (see the next Lemma 2.40), say $\mathfrak{a}_i \subset \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_k$. Then \mathfrak{m} is an accumulation point of \mathfrak{a}_i if any neighborhood of \mathfrak{m} contains all the ideals \mathfrak{m}_i , $1 \leq i \leq k$. But this is impossible! In fact, for example the neighborhood $U_1 = \text{Spec}(\mathbb{Z}_r) \setminus \mathfrak{m}_1$ of \mathfrak{m} cannot contain \mathfrak{m}_1 . \square

Lemma 2.37 (Decompositions of ideals \mathfrak{a}_i in irreducible components). *Each ideal \mathfrak{a}_i in the above set $\{\mathfrak{a}_i\}$, admits an irreducible decomposition into primary ideals of \mathbb{Z}_r . If $(2n-b_i) = b_1^{r_1} \dots b_m^{r_m}$, is the prime factorization of $(2n-b_i)$, then one has the representation (20).*

$$(20) \quad \mathfrak{a}_i = \frac{b_1^{r_1} \mathbb{Z}}{r \mathbb{Z}} \cap \dots \cap \frac{b_m^{r_m} \mathbb{Z}}{r \mathbb{Z}}.$$

Furthermore, one has $\mathfrak{r}(\mathfrak{a}_i) = b_1 \dots b_m \mathbb{Z} / r \mathbb{Z}$.

If \mathfrak{a}_i is primary then $\mathfrak{r}(\mathfrak{a}_i)$ is prime. If \mathfrak{a}_i is maximal then $\mathfrak{r}(\mathfrak{a}_i) = \mathfrak{a}_i$, i.e., \mathfrak{a}_i is a radical ideal. (The converse is in general false.)

Proof. Let us recall that an ideal $\mathfrak{q} \subset R$ of a ring R , is *primary* if $xy \in \mathfrak{q}$ implies either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$, for some $n > 0$. This is equivalent to say that $R/\mathfrak{q} \neq 0$ and every zero-divisor in R/\mathfrak{q} is nilpotent. If \mathfrak{q} is primary then $\mathfrak{r}(\mathfrak{q})$ is the smallest prime ideal containing \mathfrak{q} .²¹ Furthermore an ideal $\mathfrak{q} \subset R$ is called *irreducible* if $\mathfrak{q} = \mathfrak{c} \cap \mathfrak{d}$

¹⁹ $\mathcal{O}_{\text{Spec}(\mathbb{Z}_r)}$ is the sheaf over $\text{Spec}(\mathbb{Z}_r)$, identified by \mathbb{Z}_r , since $\mathcal{O}_{\text{Spec}(\mathbb{Z}_r)}(\text{Spec}(\mathbb{Z}_r)) = \mathbb{Z}_r$. If $x = \mathfrak{b}$ is a point of $\text{Spec}(\mathbb{Z}_r)$, then $\lim_{\substack{\longrightarrow \\ U \ni x}} \mathcal{O}_{\text{Spec}(\mathbb{Z}_r)}(U) \cong (\mathbb{Z}_r)_{\mathfrak{b}}$, where the limit is made by means

of the restriction homomorphism. (See, e.g., [1].)

²⁰This property is important because it is an a-priori motivation to consider the criterion of Tab. 1 well found. In fact it shows that the ideals \mathfrak{b}_j cannot be considered on the same footing with respect to the ideals \mathfrak{a}_i . In other words the mirror symmetry is necessary to understand how the ideals \mathfrak{a}_i "converge" to the ideals \mathfrak{b}_j .

²¹For example if $R = \mathbb{Z}$ the only primary ideals are $\langle 0 \rangle$ and $\langle p^n \rangle$, with p prime.

then $\mathfrak{q} = \mathfrak{c}$ or $\mathfrak{q} = \mathfrak{d}$. Since in a Noetherian ring every ideal is a finite intersection of irreducible ideals, it follows also that each ideal \mathfrak{a}_i admits this decomposition. In fact, if $(2n - b_i) = b_1^{r_1} \cdots b_m^{r_m}$, is the prime factorization of $(2n - b_i)$, then $\mathfrak{a}_i = \frac{(2n-b_i)\mathbb{Z}}{r\mathbb{Z}}$ has the natural decomposition (20), where each ideal $\frac{(b_j^{r_j})\mathbb{Z}}{r\mathbb{Z}}$ is a primary ideal in \mathbb{Z}_r . Finally in a Noetherian ring every ideal contains a power of its radical. Therefore, $\mathfrak{r}(\mathfrak{a}_i) \supseteq \mathfrak{a}_i$ and $\mathfrak{r}(\mathfrak{a}_i)^n \subseteq \mathfrak{a}_i \subseteq \mathfrak{r}(\mathfrak{a}_i)$, for some $n > 0$. If \mathfrak{a}_i is primary, i.e., $\mathfrak{a}_i = \frac{b^s\mathbb{Z}}{r\mathbb{Z}}$, then $\mathfrak{r}(\mathfrak{a}_i) = \frac{b\mathbb{Z}}{r\mathbb{Z}} = \mathfrak{m}$, a maximal ideal of \mathbb{Z}_r and $\mathfrak{m} \supset \mathfrak{a}_i$. In fact, $\mathfrak{a}_i = \frac{\mathbb{Z}}{r'\mathbb{Z}}$ with $r'b^s = r$ and $\mathfrak{m} = \frac{\mathbb{Z}}{r''\mathbb{Z}}$ with $r''b = r$. Then $r'' > r'$ and $r''|r'$, since $r'b^s = r''b$. Therefore, $\mathfrak{a}_i = \mathbb{Z}_{r'} \subset \mathbb{Z}_{r''} = \mathfrak{m}$. \square

It is useful in these calculations to utilize the following lemma.

Lemma 2.38 (Relations between direct sum, intersection and sum of \mathbb{Z} -modules). *Let us consider \mathfrak{a}_i as sub- \mathbb{Z} -modules of the \mathbb{Z} -module \mathbb{Z}_r . Then one has the short exact sequence (21).*

$$(21) \quad 0 \longrightarrow \mathfrak{a}_i \cap \mathfrak{a}_j \xrightarrow{f} \mathfrak{a}_i \oplus \mathfrak{a}_j \xrightarrow{h_i - h_j} \mathfrak{a}_i + \mathfrak{a}_j \longrightarrow 0, \quad i \neq j$$

where $h_i : \mathfrak{a}_i \rightarrow \mathfrak{a}_i + \mathfrak{a}_j$ and $h_j : \mathfrak{a}_j \rightarrow \mathfrak{a}_i + \mathfrak{a}_j$ are the canonical injections and $f(x) = (x, x) \in \mathfrak{a}_i \oplus \mathfrak{a}_j$. Then $(h_i - h_j)(x, y) = x - y$. Furthermore, one has also the short exact sequence (22).

$$(22) \quad 0 \longrightarrow \mathbb{Z}_r / (\mathfrak{a}_i \cap \mathfrak{a}_j) \longrightarrow (\mathbb{Z}_r / \mathfrak{a}_i) \oplus (\mathbb{Z}_r / \mathfrak{a}_j) \xrightarrow{p_i - p_j} \mathbb{Z}_r / (\mathfrak{a}_i + \mathfrak{a}_j) \longrightarrow 0, \quad i \neq j$$

where $p_i : \mathbb{Z}_r / \mathfrak{a}_i \rightarrow \mathbb{Z}_r / (\mathfrak{a}_i + \mathfrak{a}_j)$ and $p_j : \mathbb{Z}_r / \mathfrak{a}_j \rightarrow \mathbb{Z}_r / (\mathfrak{a}_i + \mathfrak{a}_j)$ are the canonical projections

Proof. This lemma is a direct application of some standard results in commutative algebra. (See, e.g., [3].) \square

Example 2.39. For example by considering the next Example 2.48 relative to the case \mathbb{Z}_{28} , hence $\mathbb{Z}_r = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 5^2 \cdot 3^3$ one has for $\mathfrak{a}_i = \frac{5\mathbb{Z}}{r\mathbb{Z}}$ and $\mathfrak{a}_j = \frac{9\mathbb{Z}}{r\mathbb{Z}}$, the following \mathbb{Z} -modules:

$$\mathfrak{a}_i \cap \mathfrak{a}_j = \frac{5 \cdot 3^2 \mathbb{Z}}{r\mathbb{Z}}, \quad \mathfrak{a}_i + \mathfrak{a}_j = \mathbb{Z}_r, \quad \mathfrak{a}_i \oplus \mathfrak{a}_j = \frac{5\mathbb{Z}}{r\mathbb{Z}} \oplus \frac{9\mathbb{Z}}{r\mathbb{Z}}$$

to which corresponds the short exact sequence (23).

$$(23) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}_{11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 5 \cdot 3} & \longrightarrow & \mathbb{Z}_{11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 5 \cdot 3^2} \oplus \mathbb{Z}_{11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 5^2 \cdot 3} & \longrightarrow & \mathbb{Z}_{11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 5^2 \cdot 3^3} \longrightarrow 0 \\ & & \parallel & & \parallel & & \parallel \\ 0 & \longrightarrow & \mathfrak{a}_i \cap \mathfrak{a}_j & \xrightarrow{f} & \mathfrak{a}_i \oplus \mathfrak{a}_j & \xrightarrow{h_i - h_j} & \boxed{\mathfrak{a}_i + \mathfrak{a}_j \cong \mathbb{Z}_r} \longrightarrow 0 \end{array}$$

The sequence (23) means that $\mathfrak{a}_i \oplus \mathfrak{a}_j$ is larger than $\mathfrak{a}_i + \mathfrak{a}_j \cong \mathbb{Z}_r$. In fact, $\mathfrak{a}_i = \frac{5\mathbb{Z}}{r\mathbb{Z}}$ and $\mathfrak{a}_j = \frac{9\mathbb{Z}}{r\mathbb{Z}}$ are coprime ideals, (situation similar to Lemma 1.2), but the corresponding modules $\mathbb{Z}_{r'}$ and $\mathbb{Z}_{r''}$ have $\text{g.c.d.}(r', r'') = 15 \neq 1$, hence r' is not coprime of r'' . In other words $\mathbb{Z}_{r'} \oplus \mathbb{Z}_{r''} \not\cong \mathbb{Z}_{r' \cdot r''}$. (Lemma 2.4.) The kernel of the homomorphism $\mathfrak{a}_i \oplus \mathfrak{a}_j \rightarrow \mathfrak{a}_i + \mathfrak{a}_j$ is just the intersection $\mathfrak{a}_i \cap \mathfrak{a}_j$ that is an ideal of

\mathbb{Z}_r . The application of the short exact sequence (23) gives (24).

$$(24) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}_{5 \cdot 3^2} & \longrightarrow & \mathbb{Z}_5 \oplus \mathbb{Z}_9 & \longrightarrow & 0 \longrightarrow 0 \\ & & \parallel & & \parallel & & \parallel \\ 0 & \longrightarrow & \mathbb{Z}_r/(\mathfrak{a}_i \cap \mathfrak{a}_j) & \longrightarrow & (\mathbb{Z}_r/\mathfrak{a}_i) \oplus (\mathbb{Z}_r/\mathfrak{a}_j) & \xrightarrow{p_i - p_j} & \mathbb{Z}_r/(\mathfrak{a}_i + \mathfrak{a}_j) \longrightarrow 0 \end{array}$$

This just means that $\mathbb{Z}_{45} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_9$, i.e., it agrees with Lemma 2.4 since 5 and 9 are coprimes.

Lemma 2.40 (Ideals \mathfrak{a}_i and maximal ideals in \mathbb{Z}_r). *Each ideal \mathfrak{a}_i is contained into the intersection of some maximal ideals $\mathfrak{m}_i \subset \mathbb{Z}_r$, hence is contained in some maximal ideal of \mathbb{Z}_r .*

Proof. Let $\mathfrak{a}_i = \frac{(2n-b_i)\mathbb{Z}}{r\mathbb{Z}}$. If $(2n-b_i) = b_j$, then \mathfrak{a}_i is maximal! Let us assume that $(2n-b_i) = a_i$ is not prime. Then one has that \mathfrak{a}_i is contained in the intersection of primary ideals. This follows from the fact that \mathbb{Z}_r is a Noetherian ring. However, let us look directly this property. In fact, if $(2n-b_i) = a_i$ admits the following prime factorization $(2n-b_i) = a_i = b_1^{r_1} \cdots b_k^{r_k}$, then one has the following isomorphisms

$$\mathfrak{a}_i = \frac{b_1^{r_1} \cdots b_k^{r_k} \mathbb{Z}}{r\mathbb{Z}} = \frac{b_1^{r_1} \mathbb{Z}}{r\mathbb{Z}} \cap \cdots \cap \frac{b_k^{r_k} \mathbb{Z}}{r\mathbb{Z}} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k$$

where $\mathfrak{p}_m = \frac{b_m^{r_m} \mathbb{Z}}{r\mathbb{Z}}$, $1 \leq m \leq k$, are primary ideals in \mathbb{Z}_r . One has also the following inclusions and isomorphisms:

$$\mathfrak{a}_i \subset \mathfrak{r}(\mathfrak{a}_i) = \frac{b_1 \cdots b_k \mathbb{Z}}{r\mathbb{Z}} = \frac{b_1 \mathbb{Z}}{r\mathbb{Z}} \cap \cdots \cap \frac{b_k \mathbb{Z}}{r\mathbb{Z}} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k.$$

□

Example 2.41. Let us look to the case $2n = 220$, reported in Tab. 1. Let us consider only the ideals $\mathfrak{a}_i = \frac{(2n-b_i)\mathbb{Z}}{r\mathbb{Z}}$ corresponding to the steps reported in Tab. 1. Then one has the relation between ideals \mathfrak{a}_i and maximal ideals in \mathbb{Z}_r reported in Tab. 5.

TABLE 5. Some examples of maximal ideals containing some ideals \mathfrak{a}_i in the case $2n = 220$.

$\mathfrak{a}_1 = (220 - 211)\mathbb{Z}/r\mathbb{Z} = 3^2\mathbb{Z}/r\mathbb{Z} \subset 3\mathbb{Z}/r\mathbb{Z} = \mathfrak{m}_1 = \mathfrak{r}(\mathfrak{a}_1)$
$\mathfrak{a}_2 = (220 - 199)\mathbb{Z}/r\mathbb{Z} = 3 \cdot 7\mathbb{Z}/r\mathbb{Z} = (3\mathbb{Z}/r\mathbb{Z}) \cap (7\mathbb{Z}/r\mathbb{Z}) = \mathfrak{m}_1 \cap \mathfrak{m}_2 = \mathfrak{r}(\mathfrak{a}_2)$
$\mathfrak{a}_3 = (220 - 197)\mathbb{Z}/r\mathbb{Z} = 23\mathbb{Z}/r\mathbb{Z} = \mathfrak{m}_6 = \mathfrak{r}(\mathfrak{a}_3)$

See also Tab. 1.

$r = l.c.m.(a_i)$.

$\mathbb{Z}_{220}^\times = \{1, a_i \mid 1 < a_i < 220 = 2^2 \cdot 5 \cdot 11, g.c.d.(220, a_i) = 1\}$.

Maximal ideals in \mathbb{Z}_r : $\{\mathfrak{m}_i\} = \{\frac{3\mathbb{Z}}{r\mathbb{Z}}, \frac{7\mathbb{Z}}{r\mathbb{Z}}, \frac{13\mathbb{Z}}{r\mathbb{Z}}, \frac{17\mathbb{Z}}{r\mathbb{Z}}, \frac{19\mathbb{Z}}{r\mathbb{Z}}, \frac{23\mathbb{Z}}{r\mathbb{Z}}, \dots\}$.

Example 2.42. In Tab. 6 are reported the relations between ideals \mathfrak{a}_i and maximal ideals \mathfrak{m}_j in \mathbb{Z}_r , for the case $2n = 28$, considered also in the next Example 2.48.

In order to conclude this proof, i.e., to assure that in the set $\{\mathfrak{a}_i\}$ are also included maximal ideals of the type $\mathfrak{m} = b\mathbb{Z}/r\mathbb{Z} \subset \mathbb{Z}_r$, the following lemma give the definite answer.

TABLE 6. Examples of maximal ideals containing ideals \mathfrak{a}_i in the case $2n = 28$.

$\mathfrak{a}_1 = (2n - 23)\mathbb{Z}/r\mathbb{Z} = 5\mathbb{Z}/r\mathbb{Z} = \mathfrak{m}_2 = \mathfrak{r}(\mathfrak{a}_1)$
$\mathfrak{a}_2 = (2n - 19)\mathbb{Z}/r\mathbb{Z} = 3^2\mathbb{Z}/r\mathbb{Z} \subset \mathfrak{m}_1 = \mathfrak{r}(\mathfrak{a}_2)$
$\mathfrak{a}_3 = (2n - 17)\mathbb{Z}/r\mathbb{Z} = 11\mathbb{Z}/r\mathbb{Z} = \mathfrak{m}_3 = \mathfrak{r}(\mathfrak{a}_3)$
$\mathfrak{a}_4 = (2n - 13)\mathbb{Z}/r\mathbb{Z} = 3 \cdot 5\mathbb{Z}/r\mathbb{Z} = \mathfrak{m}_1 \cap \mathfrak{m}_2 = \mathfrak{r}(\mathfrak{a}_4)$
$\mathfrak{a}_5 = (2n - 11)\mathbb{Z}/r\mathbb{Z} = 17\mathbb{Z}/r\mathbb{Z} = \mathfrak{m}_5 = \mathfrak{r}(\mathfrak{a}_5)$
$\mathfrak{a}_6 = (2n - 5)\mathbb{Z}/r\mathbb{Z} = 23\mathbb{Z}/r\mathbb{Z} = \mathfrak{m}_7 = \mathfrak{r}(\mathfrak{a}_6)$
$\mathfrak{a}_7 = (2n - 3)\mathbb{Z}/r\mathbb{Z} = 5^2\mathbb{Z}/r\mathbb{Z} \subset \mathfrak{m}_2 = \mathfrak{r}(\mathfrak{a}_7)$

See also Example 2.48.

$$r = l.c.m.(a_i) = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 25 \cdot 27.$$

$$\mathbb{Z}_{28}^\times = \{1, a_i \mid 1 < a_i < 28 = 2^2 \cdot 7, g.c.d.(28, a_i) = 1\}.$$

Maximal ideals in \mathbb{Z}_r :

$$\{\mathfrak{m}_i\} = \left\{ \frac{3\mathbb{Z}}{r\mathbb{Z}}, \frac{5\mathbb{Z}}{r\mathbb{Z}}, \frac{11\mathbb{Z}}{r\mathbb{Z}}, \frac{13\mathbb{Z}}{r\mathbb{Z}}, \frac{17\mathbb{Z}}{r\mathbb{Z}}, \frac{19\mathbb{Z}}{r\mathbb{Z}}, \frac{23\mathbb{Z}}{r\mathbb{Z}} \right\}.$$

Lemma 2.43 (Goldbach bordism and Goldbach couples). *The set of ideals $\{\mathfrak{a}_i\}$ contains a maximal ideal of \mathbb{Z}_r at least.*

Proof. Let us consider the natural embeddings $\mathbb{Z} \rightarrow \mathbb{R} \rightarrow \mathbb{R}^2$, $n \mapsto n \mapsto (n, 0)$. Then we say that a couple of points $a, b \in \mathbb{R}^2$ are *2n-Goldbach bording* if there exists a smooth curve $\gamma : [0, 1] \rightarrow \mathbb{R}^2$ such that $\gamma(0) = a$, $\gamma(1) = b$ and γ intersects the straight-line of \mathbb{R}^2 , identified by these two points, into a couple of integers $\bar{a}, \bar{b} \in \mathbb{Z} \subset \mathbb{R}$, such that (\bar{a}, \bar{b}) is a Goldbach couple with respect to an even integer $2n$. In particular (\bar{a}, \bar{b}) can be also a trivial Goldbach couple, i.e., (\bar{a}, \bar{a}) , with $\bar{a} = n$ prime. Let us denote by ${}^{2n}\Omega_{GB}$ the *2n-Goldbach bordism group*. Let us prove that ${}^{2n}\Omega_{GB} = \mathbb{Z}_2$, i.e., any two points in \mathbb{R}^2 are 2n-Goldbach bording, for $n \geq 1$. In the short exact sequence (25) is reported the relation between ${}^2\Omega_{GB}$ and non-oriented 0-bordism in \mathbb{R}^2 .

$$(25) \quad 0 \longrightarrow \ker({}^2b) \longrightarrow {}^2\Omega_{GB} \xrightarrow{{}^2b} \boxed{\Omega_0(\mathbb{R}^2) \cong \mathbb{Z}_2} \longrightarrow 0$$

In fact, given two points $a, b \in \mathbb{R}^2$, we can assume that they are on the x -axis and by a further transformation to assume that $a = 0$ and $b = 2$. Then the curve $y = \sin(\hat{x})$ with $\hat{x} = x/\pi$, passes for $\hat{x} = 0$ for a and for $\hat{x} = 2$ for b and has a further zero at $\hat{x} = 1$. This identifies the trivial Goldbach couple $(1, 1)$ for the even number $2n = 2$. Therefore the two points a and b are 2-Goldbach bording. Since these are arbitrary points in \mathbb{R}^2 , it follows that $\ker({}^2b) = 0$, hence ${}^2\Omega_{GB} \cong \Omega_0(\mathbb{R}^2)$. This conclusion can be generalized to any even number $2n$. In fact one can consider the mapping ${}^{2n}f : x \mapsto \hat{x} = x/n\pi$, that transforms the interval $[0, 2n\pi]$ into $[0, 2]$ and the points $a = 0$ and $b = 2n\pi$ into the points $\hat{x} = 0$ and $\hat{x} = 2$ respectively. Furthermore the point $x = \pi n$ is transformed into $\hat{x} = 1$. Then the curve $y = \sin(\hat{x})$ realizes again the 2-Goldbach bordism. On the other hand one has the induced homomorphism ${}^{2n}\Omega_{GB} \rightarrow {}^2\Omega_{GB}$ on the Goldbach bordism groups. More precisely one has the exact commutative diagram (26).²²

²²Warn ! A priori we cannot know the structure of the $2n$ -Goldbach bordism group, but the mapping ${}^{2n}f$ allows us to relate it to the 2-Goldbach bordism group. In fact, the mapping ${}^{2n}f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is a diffeomorphism, since it is represented by the functions $({}^{2n}f^1, {}^{2n}f^2) = (x, y) = (x1, x^2) \mapsto (\hat{x} = \frac{x}{\pi n}, y)$. The corresponding jacobian matrix is $(\partial x_k, {}^{2n}f^j) = \begin{pmatrix} 1/\pi n & 0 \\ 0 & 1 \end{pmatrix}$ with

$$(26) \quad \begin{array}{ccccccc} & & 0 & & 0 & & \\ & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & {}^{2n}\Omega_{GB} & \xrightarrow{{}^{2n}b} & \boxed{\Omega_0(\mathbb{R}^2) \cong \mathbb{Z}_2} & \longrightarrow & 0 \\ & & \uparrow {}^{2n}f_* & & \uparrow {}^{2n}f_* & & \\ 0 & \longrightarrow & {}^{2n}\Omega_{GB} & \xrightarrow{{}^{2n}b} & \boxed{\Omega_0(\mathbb{R}^2) \cong \mathbb{Z}_2} & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \\ & & 0 & & 0 & & \end{array}$$

The homomorphism ${}^{2n}f_* : {}^{2n}\Omega_{GB} \rightarrow {}^{2n}\Omega_{GB}$ is an isomorphism for construction and the homomorphism ${}^{2n}b : {}^{2n}\Omega_{GB} \rightarrow \Omega_0(\mathbb{R}^2)$ is also an isomorphism since ${}^{2n}\Omega_{GB} \cong \Omega_0(\mathbb{R}^2) \cong \Omega_0(\mathbb{R}^2)$ are isomorphisms. Therefore, one has the isomorphism ${}^{2n}\Omega_{GB} \cong \mathbb{Z}_2$. As a by product we get that in the set of ideals $\{\mathfrak{a}_i\}$ there exists a maximal one at least, $\mathfrak{m} = b\mathbb{Z}/r\mathbb{Z}$, with $b_j = 2n - b_i$ prime and b_i a prime of the interval $]1, 2n[\subset \mathbb{N}$ identifying a strong generator in \mathbb{Z}_{2n} . \square

In order to avoid any possible confusion, let us apply the proof to some significative examples.

Example 2.44 ($\boxed{2n = 2}$). In this case there exists the canonical Noether Goldbach couple $(1, 2n - 1) = (1, 1)$. This is a trivial Goldbach couple, since $n = 1$ is prime. The set of ideals $\{\mathfrak{a}_i\} = \emptyset$.

Example 2.45 ($\boxed{2n = 6}$). In this case there exists the canonical Noether Goldbach couple $(1, 2n - 1) = (1, 5)$. Since $n = 3$ is prime there exists also the trivial Goldbach couple $(3, 3)$. Then $\{\mathfrak{a}_i\} = \emptyset$. Therefore, do not exist other Goldbach couples.

Example 2.46 ($\boxed{2n = 8}$). In this case there exists the canonical Noether Goldbach couple $(1, 2n - 1) = (1, 7)$. Instead does not exist the trivial Goldbach couple since $n = 4$ is even. $r = \text{l.c.m.}(3, 5) = 15$.

$$\{\mathfrak{a}_i\} = \left\{ \frac{(2n - 5)\mathbb{Z}}{15\mathbb{Z}}, \frac{(2n - 3)\mathbb{Z}}{15\mathbb{Z}} \right\} = \left\{ \frac{3\mathbb{Z}}{15\mathbb{Z}}, \frac{5\mathbb{Z}}{15\mathbb{Z}} \right\}.$$

The set of maximal ideals is

$$\{\mathfrak{m}_i\} = \left\{ \mathfrak{m}_1 = \frac{3\mathbb{Z}}{15\mathbb{Z}}, \mathfrak{m}_2 = \frac{5\mathbb{Z}}{15\mathbb{Z}} \right\},$$

to which corresponds the same Goldbach couple $(3, 5)$. By summarizing, the Goldbach couples in \mathbb{Z}_8 are $(1, 7)$ and $(3, 5)$.

Example 2.47 ($\boxed{2n = 10}$). In this case does not exist the canonical Noether Goldbach couple, since $2n - 1 = 9$ is not a prime number, but there exists the trivial Goldbach couple $(5, 5)$, since n is prime. $r = \text{l.c.m.}(3, 7) = 21$.

$$\{\mathfrak{a}_i\} = \left\{ \frac{(2n - 7)\mathbb{Z}}{21\mathbb{Z}}, \frac{(2n - 3)\mathbb{Z}}{21\mathbb{Z}} \right\} = \left\{ \frac{3\mathbb{Z}}{21\mathbb{Z}}, \frac{7\mathbb{Z}}{21\mathbb{Z}} \right\}.$$

$\det(\partial x_k, {}^{2n}f^j) = 1/\pi n \neq 0$. Thus we can consider the inverse diffeomorphism ${}^{2n}f^{-1} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ and we necessarily get ${}^{2n}\Omega_{GB} \cong {}^{2n}f_*^{-1}({}^{2n}\Omega_{GB})$.

The set of maximal ideals is

$$\{\mathfrak{m}_i\} = \{\mathfrak{m}_1 = \frac{3\mathbb{Z}}{21\mathbb{Z}}, \mathfrak{m}_2 = \frac{7\mathbb{Z}}{21\mathbb{Z}}\}.$$

To \mathfrak{m}_1 and \mathfrak{m}_2 corresponds the same Goldbach couple $(3, 7)$. By summarizing the Goldbach couple in \mathbb{Z}_{10} is $(3, 7)$. To this must be added the trivial Goldbach couple $(5, 5)$ that does not come from units in \mathbb{Z}_{10} .

Example 2.48 ($\boxed{2n = 28}$). In this case does not exist a canonical Noether Goldbach couple, since $2n - 1 = 27$ is not a prime number, and neither there exists a trivial Goldbach couple, since $n = 14$ is not prime.

$$r = \text{l.c.m.}(3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27) = 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 25 \cdot 27 = 717084225.$$

$$\begin{cases} \{\mathfrak{a}_i\} &= \left\{ \frac{(2n-23)\mathbb{Z}}{r\mathbb{Z}}, \frac{(2n-19)\mathbb{Z}}{r\mathbb{Z}}, \frac{(2n-17)\mathbb{Z}}{r\mathbb{Z}}, \frac{(2n-13)\mathbb{Z}}{r\mathbb{Z}}, \frac{(2n-11)\mathbb{Z}}{r\mathbb{Z}}, \frac{(2n-5)\mathbb{Z}}{r\mathbb{Z}}, \frac{(2n-3)\mathbb{Z}}{r\mathbb{Z}} \right\} \\ &= \left\{ \frac{5\mathbb{Z}}{r\mathbb{Z}}, \frac{9\mathbb{Z}}{r\mathbb{Z}}, \frac{11\mathbb{Z}}{r\mathbb{Z}}, \frac{15\mathbb{Z}}{r\mathbb{Z}}, \frac{17\mathbb{Z}}{r\mathbb{Z}}, \frac{23\mathbb{Z}}{r\mathbb{Z}}, \frac{25\mathbb{Z}}{r\mathbb{Z}} \right\}. \end{cases}$$

The set of maximal ideals of \mathbb{Z}_r , belonging to the set $\{\mathfrak{a}_i\}$ is the following:²³

$$\{\mathfrak{m}_i\} = \{\mathfrak{m}_2 = \frac{5\mathbb{Z}}{r\mathbb{Z}}, \mathfrak{m}_3 = \frac{11\mathbb{Z}}{r\mathbb{Z}}, \mathfrak{m}_5 = \frac{17\mathbb{Z}}{r\mathbb{Z}}, \mathfrak{m}_7 = \frac{23\mathbb{Z}}{r\mathbb{Z}}\}.$$

To \mathfrak{m}_2 and \mathfrak{m}_7 corresponds the same Goldbach couple $(5, 23)$ and to \mathfrak{m}_3 and \mathfrak{m}_5 there corresponds the Goldbach couple $(11, 17)$.

In conclusion, in the ring \mathbb{Z}_{2n} there exists a canonical Goldbach couple, and this can be found by means of the criterion in Tab. 1. The same criterion allows us to find also all the other Goldbach couples. Therefore, the proof of the Theorem 2.20 is done ! \square

Corollary 2.49 (Goldbach Conjecture). Any even integer $2n$, $n \geq 1$, can be split into the sum of two primes p_1 and p_2 : $2n = p_1 + p_2$.²⁴

Corollary 2.50 (Restricted Goldbach Conjecture). Any even integer $2n$, $n > 1$, can be split into the sum of two primes p_1 and p_2 : $2n = p_1 + p_2$.²⁵

²³Compare with Tab. refexamples-maximal-ideals-containing-ideals-ai-case-2n-28.

²⁴Let us emphasize that n can be any integer ≥ 1 . In fact, if n is a prime number, it is trivial that $2n$ is the sum of two primes: $2n = n + n$.

²⁵Let us underline that the GC in its original form considers 1 as a prime number ! More recently, a restricted version of GC, (say RGC), has been proposed by assuming the restricted prime numbers set $P^\bullet = P \setminus \{1\}$ only, and even numbers $2n$, with $n > 1$. So to the RGC it should appear applicable the Gödel incompleteness theorem, with respect to the criterion in Tab. 1 adopted to prove the GC. On the other hand our proof of the GC can be adapted also to prove the RGC. In fact, this is the GC with the additional restriction that the Noether Goldbach couples cannot be considered as acceptable solutions. However, Noether Goldbach couples are found simply by looking to the fact if $2n - 1$ are primes or not. So, identified at the beginning, in the process of the criterion of Tab. 1. Really, this criterion becomes interesting just when do not exist the canonical Noether Goldbach couples. In fact, the maximal ideal $\mathfrak{m} = b\mathbb{Z}/r\mathbb{Z}$ considered in the proof of the GC, associated to the set of ideals $\mathfrak{a}_i = (2n - b_i)\mathbb{Z}/r\mathbb{Z} \subset \mathbb{Z}_r$, necessarily has $b \neq 1$.

3. Applications

In this section we give some applications interesting the classical Euclidean geometry and the quantum algebra in the sense introduced by A. Prástaro. (See [12, 13] and related Prástaro's works quoted therein.)

Proposition 3.1 (Goldbach triangle). *In a circle Γ of radius $n \in \mathbb{N}$, there exists an inscribed right triangle ABC , with hypotenuse AB passing for the centre O of Γ , such that the projection H of the vertex C on AB , divides AB into two segments AH and HB of length respectively p_1 and p_2 , prime numbers.²⁶*

In the following we give an application of the GC to the quantum algebra, in the sense of A. Prástaro [13].

Theorem 3.2 (Quantum algebraic interpretation of the Goldbach conjecture).
 • Let A be a quantum algebra in the sense of A. Prástaro, then there exists the canonical homomorphism (27), (quantum-Goldbach-homomorphism).

$$(27) \quad \begin{cases} g_* : 2\mathbb{Z} \otimes_{\mathbb{Z}} A \rightarrow \mathbb{Z}_2 \otimes_{\mathbb{Z}} A \oplus \mathbb{Z}_2 \otimes_{\mathbb{Z}} A \\ g_*(2n \otimes a) = ([p_1] \otimes a, [p_2] \otimes a) \in (1 \otimes a, 1 \otimes a) \end{cases}$$

where (p_1, p_2) is the Goldbach couple identified by the criterion reported in Tab. 1 and codified by Theorem 2.20. We call $2\mathbb{Z} \otimes_{\mathbb{Z}} A$ the (additive) group of quantum extended even-numbers. Furthermore one has the commutative diagram (28), with exact vertical line.

$$(28) \quad \begin{array}{ccc} & & 0 \\ & & \downarrow \\ & & 2\mathbb{Z} \otimes_{\mathbb{Z}} A \\ & \swarrow g_* & \downarrow b \\ \boxed{\mathbb{Z}_2 \otimes_{\mathbb{Z}} A \oplus \mathbb{Z}_2 \otimes_{\mathbb{Z}} A} & & \boxed{\mathbb{Z} \otimes_{\mathbb{Z}} A \cong A} \\ & \searrow + & \downarrow c \\ & & \mathbb{Z}_2 \otimes_{\mathbb{Z}} A \\ & & \downarrow \\ & & 0 \end{array}$$

One has the canonical isomorphisms reported in (29).

$$(29) \quad \begin{cases} \text{im}(b) \cong 2\mathbb{Z} \otimes_{\mathbb{Z}} A \cong \ker(c) \\ \text{im}(c) \cong \mathbb{Z} \otimes_{\mathbb{Z}} A / 2\mathbb{Z} \otimes_{\mathbb{Z}} A \cong \mathbb{Z}_2 \otimes_{\mathbb{Z}} A \end{cases}$$

²⁶For details on this geometric interpretation of the GC see [10], where it is emphasized the equivalence of the GC and the solution of the following Diophantine equation: $n^2 = a^2 + b^2$, where n, a and b are three integers such that $a = p_1 p_2$ and $2b = p_2 - p_1$, with p_1 and p_2 , prime numbers. This relates the GC to a *Fermat like theorem*. Let us recall that in 1900, David Hilbert proposed the solvability of all Diophantine problems as the tenth of his celebrated problems. However, after 70 years has been published a result in mathematical logic that in general Diophantine problems are unsolvable. (Matiyasevich's theorem [9].) Therefore, this proof of the Goldbach's conjecture is also an encouragement to mathematicians to solve problems, even if their solutions could have fat chance according to some general statement in mathematical logic ! (See also [7] for general information on Diophantine equations and [14] for the undecibility of these equations.)

- The quantum-Goldbach-homomorphism gives a relation between number theory, crystallographic groups and integral bordism groups of PDEs and quantum PDEs.

Proof. Let us first consider the following free resolution of the \mathbb{Z} -module \mathbb{Z}_2 :

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}_2 \longrightarrow 0$$

By tensoring this sequence with a quantum algebra A , considered as a \mathbb{Z} -module by means of the embeddings $\mathbb{Z} \rightarrow \mathbb{K} \rightarrow A$, where $\mathbb{K} = \mathbb{R}$, or $\mathbb{K} = \mathbb{C}$, we get the exact sequence (30).

(30)

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \text{Tor}^{\mathbb{Z}}(A; \mathbb{Z}) & \longrightarrow & \text{Tor}^{\mathbb{Z}}(A; \mathbb{Z}) & \longrightarrow & \text{Tor}^{\mathbb{Z}}(A; \mathbb{Z}_2) & \longrightarrow & A \otimes_{\mathbb{Z}} \mathbb{Z} & \longrightarrow & A \otimes_{\mathbb{Z}} \mathbb{Z} & \longrightarrow & A \otimes_{\mathbb{Z}} \mathbb{Z}_2 & \longrightarrow & 0 \\ & & \parallel & & \parallel & & \parallel & & \parallel & & \parallel & & \parallel & & \\ 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \text{Tor}^{\mathbb{Z}}(A; \mathbb{Z}_2) & \longrightarrow & A & \xrightarrow{2} & A & \longrightarrow & A \otimes_{\mathbb{Z}} \mathbb{Z}_2 & \longrightarrow & 0 \end{array}$$

From the bottom horizontal line, we can calculate $\text{Tor}^{\mathbb{Z}}(A; \mathbb{Z}_2) = \ker(A \xrightarrow{2} A)$.

Since A is a \mathbb{K} -vector space, it follows that $\ker(A \xrightarrow{2} A) = \{0\}$. Similarly, by working with the following free resolution of \mathbb{Z} -module \mathbb{Z}_2 :

$$0 \longrightarrow 2\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}_2 \longrightarrow 0$$

we get the vertical exact sequence in (28). This is connected with the quantum-Goldbach-homomorphism. In fact, we have $+ \circ g_* = c \circ b$. Then the isomorphisms reported in (29) are directly obtained from standard algebraic considerations on the vertical exact sequence in (28).

Finally the quantum Goldbach homomorphism allows us to represent the group of quantum extended even-numbers into a quantum extension of the crystallographic group $p4m = \mathbb{Z}^2 \rtimes D_4$. In fact, $D_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ is the point group of $p4m$. On the other hand $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ can be interpreted also as integral bordism groups of some PDEs. (See [12, 13] and some Prástaro's works, quoted therein on the relation between integral bordism groups of PDEs and quantum PDEs and crystallographic groups.) \square

REFERENCES

- [1] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, London 1969.
- [2] N. Bourbaki, *Éléments de Mathématique. Algèbre I. Chapitres 1 à 3.*, Hermann, Paris 1970.
- [3] N. Bourbaki, *Éléments de Mathématique. Algèbre Commutative*, Hermann, Paris 1961–65.
- [4] K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I.*, Monatshefte für Mathematik und Physik **38**(1931), 173–98.
- [5] K. Gödel, *On Formally Undecidable Propositions of Principia Mathematica and Related Systems*, Dover, 1962.
- [6] K. Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I.* In Solomon Feferman, editor. Kurt Gödel Collected Works, volume 1, pages 144–195, Oxford University Press, 1986. German text, parallel English translation.
- [7] M. Hazewinkel, *Diophantine equations*, in Encyclopedia of Mathematics, Springer, 2001. ISBN978-1-55608-010-4.
- [8] M. Hirzel, *On formally undecidable propositions of Principia Mathematica and related systems I.* A modern translation by Hirzel.
- [9] Yu. Matiyasevich, *Enumerable sets are Diophantine*, Soviet. Mathematics **11**(2)(1970), 354–357.

- [10] K. Nambiar, *Geometrical equivalents of Global conjecture and Fermat like theorem*, [arXiv:math/021161](#) [[math.GM](#)] .
- [11] E. Noether, *Ideal Theorie in Ringbereichen*, Mathematische Annalen **83**(1)(1921), 24–66.
- [12] A. Prástaro, *Extended crystal PDE's*, [arXiv:0811.3693](#) [[math.AT](#)] .
- [13] A. Prástaro, *Quantum extended crystal super PDE's*, Nonlinear Analysis. Real World Appl. **13**(6)(2012), 2491–2529. DOI: 10.1016/j.nonrwa.2012.02.014. [arXiv:0906.1363](#) [[math.AT](#)] .
- [14] Z-W. Sun, *Reduction of unknowns in Diophantine representations*, Sci. China Ser. A **35**(3)(1992), 257-269.